

CAI  
Z1  
-2006  
I050

V.2

Government  
Publications

**Commission of Inquiry  
into the Investigation of the  
Bombing of Air India Flight 182**

3 1761 11651449 8

**Research Papers  
Volume 2  
Terrorism Financing, Charities,  
and Aviation Security**





Digitized by the Internet Archive  
in 2023 with funding from  
University of Toronto

<https://archive.org/details/31761116514498>



Commission  
of Inquiry into  
the Investigation  
of the Bombing of  
Air India Flight 182



Commission d'enquête  
relative aux mesures  
d'investigation prises à  
la suite de l'attentat à la  
bombe commis contre  
le vol 182 d'Air India

The opinions expressed in these academic studies are those of the authors;  
they do not necessarily represent the views of the Commissioner.



©Her Majesty the Queen in Right of Canada, represented by the  
Minister of Public Works and Government Services, 2010

Cat. No: CP32-89/5-2010E  
ISBN: 978-0-660-19984-9

Available through your local bookseller or through  
Publishing and Depository Services  
Public Works and Government Services Canada  
Ottawa, Ontario  
K1A 0S5

Telephone: (613) 941-5995 or 1 800 635-7943  
Fax: (613) 954-5779 or 1 800 565-7757  
[publications@pwgsc.gc.ca](mailto:publications@pwgsc.gc.ca)  
Internet: [www.publications.gc.ca](http://www.publications.gc.ca)



**Commission of Inquiry  
into the Investigation of the  
Bombing of Air India Flight 182  
Research Studies – Volume 2**

**Terrorism Financing, Charities, and Aviation Security**





## Table of Contents

<b>Kent Roach</b>	"Introduction"	7
<b>Nikos Passas</b>	"Understanding Terrorism Financing"	15
<b>Anita Indira Anand</b>	"An Assessment of the Legal Regime Governing the Financing of Terrorist Activities in Canada"	119
<b>Mark Sidel</b>	"Terrorist Financing and the Charitable Sector: Law and Policy in the United Kingdom, the United States and Australia"	155
<b>David G. Duff</b>	"Charities and Terrorist Financing: A Review of Canada's Legal Framework"	199
<b>Kathleen Sweet</b>	"Canadian Airport Security Review"	245

Table of Contents	
Part I: Introduction	1
Part II: Terrorism Financing	15
Part III: Charities	35
Part IV: Aviation Security	55
Part V: Conclusion	75



## Introduction

Kent Roach

### The Commission's Research Program

Shortly after the appointment of the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, a decision was made by the Commissioner, commission counsel and the research directors to commission a number of research papers on matters relevant to the Commission's broad mandate.

Research studies have long been an important part of the commission of inquiry process in Canada. For example, the McDonald Commission of Inquiry that examined certain activities of the Royal Canadian Mounted Police (RCMP) and made recommendations that led to the creation of the Canadian Security Intelligence Service (CSIS) in 1984 issued a number of research papers and monographs as part of its process.<sup>1</sup> Other commissions of inquiry at both the federal and provincial levels have followed suit with, at times, ambitious research agendas.<sup>2</sup>

Research allows commissions of inquiry to be exposed to and informed by expert commentary. Research papers can be independently prepared by academics and other experts. The parties and the public are free to comment on these papers and the Commissioner is free to reject or to accept any advice provided in the research papers. The traditional disclaimer that the research paper does not necessarily represent the views of the Commission or the Commissioner is true.

The Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 faced the challenge of a particularly broad mandate that spanned the issues of the adequacy of threat assessment of terrorism both in 1985 and today, co-operation between governmental departments including the RCMP and CSIS, the adequacy of restraints on

---

<sup>1</sup> For example, see the research studies published by the McDonald Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police. J. L. J. Edwards *Ministerial responsibility for national security as it relates to the offices of Prime Minister, Attorney General and Solicitor General of Canada* (Ottawa: Supply and Services Canada, 1980); C.E.S. Franks *Parliament and Security Matters* (Ottawa: Supply and Services Canada, 1980); M.L. Friedland *National Security: The Legal Dimensions* (Ottawa: Supply and Services, 1980).

<sup>2</sup> The Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar published a series of background papers. *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services, 2006).

terrorism financing including funding from charities, witness protection, aviation security and terrorism prosecutions. A broad range of expertise drawn from a variety of academic disciplines was needed to address this mandate.

A commission of inquiry's research program can help create or solidify a research foundation for continued thought and policy development in the area being examined. Canadian research into terrorism-related issues has generally been relatively sparse.<sup>3</sup> There is no dedicated governmental funding for research related to the study of terrorism and optimal counter-terrorism measures as there is in other fields such as military studies. One of my hopes is that the research program of this Commission will stimulate further investment in independent research related to terrorism and counter-terrorism.

The Commission of Inquiry was fortunate to be able to retain the majority of Canada's leading experts in many of these areas. The Commission was also able to retain a number of leading international experts to provide research of a more comparative nature. The comparative research was undertaken to determine if Canada could learn from the best practices of other democracies in many of the areas related to its mandate.

Researchers who conduct studies for a Commission of Inquiry do not have the luxury that an academic researcher normally has in conducting research and publishing his or her work. They must work under tight deadlines and strive to produce analysis and recommendations that are of use to the Commission of Inquiry.

A decision was made to ask our researchers to write using information from public sources only, and indeed to write and complete papers long before the Commission's hearing process was completed. This means that the researchers may not always have had the full range of information and evidence that was available to the Commission. That said, the research papers, combined with the dossiers issued by commission counsel, provided the commissioner, the parties and the public with an efficient snapshot of the existing knowledge base.

---

<sup>3</sup> On some of the challenges see Martin Rudner "Towards a Proactive All-of-Government Approach to Intelligence-Led Counter-Terrorism" and Wesley Wark "The Intelligence-Law Enforcement Nexus" in Vol 1 of the Research Studies.



Because of the importance of public and party participation in this Commission of Inquiry, a decision was made early on that the researchers retained by the Commission would, whenever possible, present and defend the results of their research in the Commission's hearings. A deliberate decision was made to reject the dichotomy of part one hearings focused on the past and part two processes aimed at the future. This decision reflected the fact that much of the Commission's mandate required an examination of both the past and the future. There was also a concern that the Commissioner should be able to see the research produced for him challenged and defended in a public forum.

It is my hope that the research program will help inform the deliberations of the commission and also provide a solid academic foundation for the continued study in Canada of terrorism and the many policy instruments that are necessary to prevent and prosecute terrorism.

## **The Research Studies in this Volume**

The research studies in this volume address that part of the Commission's terms of reference which direct it that determine "whether Canada's existing legal framework provides adequate constraints on terrorist financing in, from or through Canada, including constraints on the use or misuse of funds from charitable organizations."<sup>4</sup> A final research study addresses some of the aviation security issues in the Commission's terms of reference including issues relating to the screening of passengers and their baggage.<sup>5</sup>

## **Nikos Passas "Understanding Terrorism Financing"**

Professor Nikos Passas, a leading expert on terrorism financing from Northeastern University in Boston, has prepared a comprehensive overview of the financing of terrorism as well as the international experience with the suppression of terrorism financing and in particular the influence of the 1999 International Convention for the Suppression of the Financing of Terrorism and Resolution 1373 of the United Nations Security Council. He argues that the financing of terrorism is difficult to understand and control in part because of the small amounts of money required to fund a deadly act of terrorism and in part because of the great variety of fund raising methods and sources.

---

<sup>4</sup> Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 *Terms of Reference* b (iv).

<sup>5</sup> Ibid b(vii)

Professor Passas details how the American 9/11 Commission dispelled a number of myths about the financing of 9/11 including the role of conflict diamonds, Somali hawala or informal value transfer systems and other terrorist groups. The 9/11 hijackers transferred the less than \$500,000 that was required to finance 9/11 by unexceptional means such as wire transfers, hand carry cash and the use of debit and credit cards. No financial institution filed a suspicious activity report. He argues that there are dangers that some forms of policing terrorism financing may be counterproductive by, for example, unnecessarily alienating ethnic communities, by adopting superficial compliance and by imposing costs that are greater than the benefits of increased regulation. He calls for an evidence based approach to counter terrorism financing that is informed by accurate intelligence about both terrorist groups and their funding and clear priorities including the use of targeted and well founded financing prosecutions against those groups judged to be of the greatest threat. He notes that such an approach will require integration between intelligence agencies and law enforcers, raising another theme that runs through many of the research studies.

### **Anita Indira Anand “An Assessment of the Legal Regime Governing the Financing of Terrorist Activities in Canada”**

Professor Anita Anand of the University of Toronto provides an overview of the various laws in Canada that govern the financing of terrorism. She notes that most of the post 9/11 law in Canada aimed at terrorism financing is designed to comply with Canada's various international obligations. She describes how the 2001 *Anti-Terrorism Act* added various offences related to terrorism financing to the *Criminal Code* as well as provisions for the freezing and forfeiture of property owned or controlled by a terrorist group and the reporting of suspicious transactions. She notes that there are areas of overlap with the *Proceeds of Crime Act* raising the issue of the need for co-ordination of enforcement efforts among police, intelligence agencies and the Financial Transactions and Reports Analysis Centre (FINTRAC).

Professor Anand proposes the need for both co-ordination and review of the efficacy of Canada's efforts to regulate terrorist financing. She discusses the need for an oversight body that would monitor both the propriety and efficacy of FINTRAC's operations. She argues that assumptions that the present regime is effective may not be warranted.



In particular she notes the danger that the present enforcement regime may impose greater costs than benefits. For example, there are broad reporting requirements that impose significant costs on third parties such as financial institutions with uncertain benefits in terms of successful terrorism financing prosecutions or other actions designed to disrupt terrorist groups and prevent terrorism. Professor Anand notes that Canada lacks the equivalent of the United States Office of Terrorism and Financial Intelligence which serves as a coordinating body in this area. She also argues that the broad brush approach to reporting can have adverse effects on privacy.

### **Mark Sidel “Terrorist Financing and the Charitable Sector: Law and Policy in the United Kingdom, the United States and Australia”**

Professor Mark Sidel of the University of Iowa and a leading authority on the law relating to charities provides a comparison of the laws in the United Kingdom, the United States and Australia as they relate to charities that may be involved in terrorism financing. He argues that states have a legitimate interest in stopping charities from being one of the funding sources for terrorism, but that they also should pursue these measures in a way that ensures the vibrancy of the charitable sector including the contributions that charities can make to human security.

Professor Sidel argues that the British approach has relied on regulation by the United Kingdom’s Charities Commission while the American approach has relied on criminal prosecutions of charities for material support of terrorism even though both countries have criminalized the financing of terrorism and also regulate charities. He provides a number of case studies of the engagement of the Charities Commission with charities suspected of supporting terrorism including its interventions in the Finsbury Park Mosque in London. He argues that the British regulatory approach is superior to the American approach in part because it can rely on a broad range of interventions including measures designed to increase transparency and accountability within the charity. The American approach has been to rely on several high profile criminal prosecutions and for the US Treasury Department to impose voluntary guidelines that have been criticized by many in the charitable sector as unrealistic. Australia’s more nascent approach lies somewhere in between the British and American responses and has so far involved the enactment of broad and often controversial new offences, but without much enforcement.

### **David G. Duff “Charities and Terrorist Financing: A Review of Canada’s Legal Framework”**

Professor David Duff of the University of Toronto provides an overview of the complex array of federal and provincial laws that govern charitable status of Canada in light of the fact that the Babbar Khalsa Society enjoyed charitable status until 1996. He starts with a discussion of how the provinces under section 92(7) of the *Constitution Act, 1867* have jurisdiction to regulate charities. Most provinces have, however, refused to exercise this jurisdiction vigorously with only Ontario enacting legislation that provides for powers for the removal of trustees and executors. The result has been that the federal government is the dominant regulatory presence even though it only has incidental powers in relation to the taxation of charities.

Professor Duff focuses on the federal regulation of charities including the tests under the *Income Tax Act* for a registered charity. He examines the process that is used for denial of charitable status and decreases in the number of applications for charitable status and actual registrations after both the 1996 revocation of the Babbar Khalsa’s charitable status and the events of 9/11. He also examines the *Charities Registration (Security Information) Act* which was enacted as part of the 2001 *Anti-Terrorism Act* and which allows charitable status to be revoked on the basis of information not necessarily disclosed to the charity. He suggests that the legislation could be made more proportionate by introduction of fault requirements or a due diligence defence. That said, he notes that no certificates have been issued under this new legislation and that a charity with links to terrorism could be decertified on other grounds. He also examines the process for information exchange about charities that may be involved with terrorism and calls for federal/provincial and international co-operation not only with respect to registered charities but also non-registered non-profit organizations that may provide funds for terrorism.

### **Kathleen Sweet “Canadian Airport Security Review”**

Kathleen Sweet who is the author of a number of books on aviation security and a leading expert in that field addresses the issues of aviation security in light of a detailed discussion of the flaws in aviation security that led to the bombing of Air India Flight 182 and the bombing three years later of Pan Am Flight 103 over Lockerbie Scotland. She notes how

after the Air India bombing, Canada was the first country to require passenger baggage reconciliation on international flights, a security measure that was later extended to domestic flights.

Ms. Sweet examines a range of aviation security measures. She stresses the problems of poor operator performance with respect to the screening of baggage and suggests that there should be a renewed emphasis on attracting the best people, training them and monitoring their job performance. She points out that the use of standard x ray screening is highly dependent on the performance of human monitors. She also examines a range of more expensive technology that can be used to screen baggage as well as the use of trained dogs which are the least expensive but often effective means of detecting explosives. She also examines passenger screening by machines designed to detect traces of explosives and the use of walk through and hand-held metal detectors. Finally, she examines a range of best practices in controlling access to airports. Ms. Sweet warns that improvement in some aspects of aviation security may make other aspects a more likely target for terrorists. In addition, existing aviation security procedures remain vulnerable to circumvention often because of a desire to ensure the efficient movement of planes, passengers and their baggage.

## **Conclusion**

The first four essays in this volume provide a valuable introduction to the many modes of funding of terrorism as well as the range of interventions that can be taken against such funding including funding that may be provided by registered charities. The essays provide important cautionary tales about how deadly acts of terrorism such as the bombing of Air India Flight 182 can be financed through small sums that can be obtained and transferred through a great variety of means. They suggest that laws against the financing of terrorism including laws that would apply to charities that finance terrorism are required, but that their administration should be proportionate, cost effective and informed by accurate information and co-ordinated with other anti-terrorism measures. The final essay in this volume examines some of the aviation security breaches that led to the bombing of Air India Flight 182 as well the range of contemporary measures that can be taken to achieve better aviation security.





**Understanding Terrorism Financing  
Report prepared for the Major  
Commission of Inquiry into the Investigation  
of the Bombing of Air India Flight 182**

**Dr. Nikos Passas  
Professor, Northeastern University**



## CONTENTS

Introduction	19
Understandings and Definitions of Terrorist Finance	23
Methods of Fundraising by Terror Groups	28
Legitimate Sources	31
Illegitimate Sources	35
Terror-Crime for Profit Typology	40
Methods of Transfer	42
Informal/Unregulated Channels	42
Formal/Regulated Means	47
Amounts Involved	51
Operating vs. Operational Costs (Acts vs. Large Groups and Infrastructures)	52
A Typology of Terrorist Groups	56
Problems with Imperfect Knowledge	58
"Conflict Diamonds" and al Qaeda: A Theory with no Empirical Support	58
Al Barakaat and Terrorism: Links Never Substantiated	62
Charities and Terrorism: Undercutting Our Own Objectives?	72
Regulatory Responses	76
Objectives and Risks of CFT	78
Cost-Benefit Analyses?	79
Are Certain Areas Overlooked or Over-Emphasized?	80
Financial Controls and Remittances	80
CFT and Trade	83
Policy implications	84
Evidence-Based CFT Policy Construction	87
Identifying the Highest Risks and Trade Transparency	91
Legitimacy of CFT	101
Conclusion	106
Appendix: Two Solutions	107
Leadminer	109
Distributed Capital	109





## Introduction

Even though this was recognized widely with some delay, financial controls are an essential and indispensable counter-terrorism tool. The utility of financial controls was first neglected, then overestimated and subsequently more reasonably considered in conjunction with the rest of our counter-terrorism arsenal.

As the day of September 11, 2001 arrived, the United Nations 1999 Convention for the Suppression of the Financing of Terrorism was awaiting ratifications and did not come into force until April 10, 2002. The USA ratified it on June 26 of that year, following a post 9/11 sense of urgency and an official policy aimed at choking off al Qaeda and other terrorists' money. A series of measures at the national, regional and international levels were introduced and enforced in an effort to deprive militants of the means to inflict serious damage.

Internationally, UN Security Council Resolutions 1267, 1373 and 1377 and initiatives from the European Union, the Financial Action Task Force (FATF) and organizations including the World Bank and the IMF have combined to raise the profile of financial controls. Consequently, a powerful arsenal has been implemented by both governments and private sector entities alert to the possibility of being abused by extremists around the world.

Six years into drastic and extensive financial controls directed at terrorist groups, one needs to assess the impact of this arsenal and whether the assumptions underlying these controls are accurate. Unfortunately, our knowledge remains incomplete, mainly due to a lack of systematic and comprehensive collection of reliable data, which could then be properly analyzed. Despite several individual cases and pieces of information or, perhaps more likely, because of our fragmented collective vision of the social organization of terrorist groups and the financial aspects of it in particular<sup>1</sup>, there are some strong controversies revolving on several issues: the role played by non-profit organizations and charities, the informal sector (compared to the formal financial system, which is presumed to be well regulated and more transparent), the trade in various commodities (especially precious stones, gold, tobacco, or counterfeit goods), the nexus between terrorist groups and 'organized crime', especially links

---

<sup>1</sup> This fragmentation is due to the parallel and at times competing activities of multiple organizations and agencies, the lack of quick and smooth sharing of information, and the absence of rigorous analysis of the available evidence scattered through various jurisdictions within the same country and around the world.

between drug trafficking and terror groups, etc.. The lack of in-depth 'peer review' and double-checking of the proliferating reports and publications in different media about terrorism have allowed inaccurate, wrong and misleading interpretations to enter into official thinking and policy planning.

Ongoing debates revolve mainly around the actual and potential sources of funds, the ways in which funds are stored or transferred, the amounts involved or required for terrorism, the ways in which national authorities and the international community can effectively respond, and the foreseeable consequences of current and proposed courses of action. Disagreements are not so much about whether this or that type of funding has been used by extremist groups. There is such a diversity of sources that one can hardly find a single way in which funds have not been raised for some militant group. The disagreements are rather about the relative extent and significance of different fund-raising methods used by specific groups. Which argument one decides to adopt has consequences on policy and security.

An argument of this report is that lofty or misguided expectations and misapplication of financial controls may be not only ineffective but also counter-productive, ultimately hurting national interests and the international community. It is, thus, imperative that we understand the limits and risks of financing controls. At the same time, it is indispensable that we fine-tune and apply them on the basis of hard data and a good understanding of the social organization<sup>2</sup> of terrorist groups. The financial aspects of terrorism are part of that social organization and require constant monitoring and attention, as they often evolve over time (also adjusting to control practices and effects). The existence of very serious disagreements on these issues so long after 9/11 shows that much more systematic and thoughtful work is required as we seek to gather valid evidence and engage in proper analysis<sup>3</sup>.

---

<sup>2</sup> That is, the division of labor, area of operations, selection of targets and methods, available resources, sympathy and support, etc.

<sup>3</sup> See, for instance, the strong critique of US policies in Naylor Naylor, R. T. (2006). *Satanic Purses: money, myth, and misinformation in the war on terror*. Montreal: McGill-Queen's University Press; the strong critique of Naylor's book by Jeff Breinholt of the US Department of Justice; the strong rejection of Rohan Gunaratna (Gunaratna, R. (2002). *Inside Al Qaeda: Global Network of Terror*. New York: Columbia University Press) as 'expert' by former US Department of Homeland Security terrorism analyst Joshua Sinai (Sinai, J. (2007). A Dubious Source: Counterterrorism Book Falls Short. *The Washington Times*(April 17), the strong critique of Gunaratna's vision of al Qaeda by Jason Burke (Burke, J. (2003). *Al-Qaeda: Casting a Shadow of Terror*. London ; New York: I.B. Tauris), the strong critique of the conflict diamonds story appearing in media, NGO and policy reports by Nikos Passas (Passas, N. (2004). *The Trade in Diamonds: Vulnerabilities for Financial Crime and Terrorist Finance*. Vienna, VA: FinCEN, US Treasury Department; Passas, N., & Jones, K. (2006). The Trade in Commodities and Terrorist Financing: Focus on Diamonds. *European Journal of Criminal Policy and Research*, 12, 1-33), etc.

This paper will hopefully provide a basis on which this debate can move forward towards a consensus-building and commonly accepted empirical ground ('consensual knowledge').

Even though this paper does not address the question of what is terrorism, the problematic nature of its definition cannot be ignored when we seek to understand the financing of terrorist groups and their operation. The point is simple and practical: if terrorism is not separated from a host of phenomena that one side or the other labels as "terrorism", then virtually all conflicts are within the scope of this report. The whole question of terrorist fundraising then becomes trite and generic: every legal and illegal source imaginable has been and can be used. Every group involved in violent conflict is bound to employ whatever means and resources are available to it.

Rebels, insurgents, resisters, guerillas, militants, militias, independence movements, nationalists etc. come in different sizes, operate in diverse contexts, enjoy differential popular (or state) support, antagonize different social actors and represent high or low priorities of domestic, regional and international controllers. Placing them all in the same category and discussing this in general terms as 'terrorist finance and its control' obscures more issues than it clarifies. Inevitably, the label 'terrorist' is a blanket political and polemical concept that varies from one legal system to another. As a result, any discussion of 'terrorist finance' is directly affected and infected by the problem of defining terrorism.

Terrorism is far from a scientific or objective term. Consequently, responses have varied from 'regime de faveur' for political offenders in olden times to regime de rigueur in recent times<sup>4</sup>. With no universally accepted definition, treatment has varied greatly from place to place and overtime. As the US National Research Council also concluded, it is simply not possible to define it<sup>5</sup>.

---

<sup>4</sup> See Passas, N. (2006). International Terrorism. In J. Greene (Ed.), *Encyclopedia of Police Science* (pp. 1267-1274). London: Routledge; Passas, N. (1986). Political Crime and Political Offender: Theory and Practice. *Liverpool Law Review*, 8(1), 23-36.

<sup>5</sup> See (US) National Research Council. (2002). *Terrorism: Perspectives from the Behavioral and Social Sciences*. Washington, D.C.: National Academies Press.



We are left with legal definitions, the work of political bodies in different countries, which still makes it a nebulous concept that is operationalized by the executive listing of concrete groups and organizations that fit the general descriptions<sup>6</sup>.

Even so, there are huge gaps and asymmetries in legal definitions, cultural understandings and actual practices. While al Qaeda has had the potential to unify the world (“Nous sommes tous americains”, read the headline in *Le Monde* after 9/11), the weight of the counter-terrorism measures has been felt by multiple other groups where matters are more complicated<sup>7</sup>.

The distinction between different types of extreme or militant groups is also critical to the effectiveness of financial controls. If we all agree that the top priority in the West is al Qaeda, then attacks on other groups less radical or less threatening to Western interests and collateral damage risk escalation, radicalization and shifts towards support of more aggressive and costlier methods by larger numbers of people. If Western countries, for example, prioritize their fight against groups such as Hizb-ut Tahrir or groups seeking independence or basic rights in Central Asia and former Soviet Republics, the risk is that non-violent or relatively moderate groups may get radicalized and some of their supporters may gradually become more prepared to use violence. As sympathizers come from different societal backgrounds, their skills and access to methods of fund raising and value transfers become so diverse and non-transparent or untraceable that both monitoring and preventing terrorism efforts are undermined.

So, even if we follow country-based legal definitions, we are still left with a very wide range of groups and organizations. For example some countries may list or classify as terrorists political dissidents, whom they try to link to enemies of other states in order to achieve strategic and tactical advantages or personal/political gains. There is a need to establish priorities for the greatest threats.

---

<sup>6</sup> The wide definition of “terrorism” by Canada and parallel listing of specific groups as terrorist in s. 83 of the Criminal Code is an innovative approach. It will be interesting to see how frequently the list may need to be amended in the light of fresh assessments of the global and domestic threats on the basis of new evidence or other considerations.

<sup>7</sup> Heated debates focus, for example, on groups such as Hamas and Hizbollah. George Soros wrote an opinion piece in April 2007 about the need to de-escalate the conflict in the Middle East through dialogue with the political side of Hamas towards a path of peace – G. Soros (2007) “On Israel, America and AIPAC”, New York Review of Books, Volume 54, Number 6.

If terrorism becomes an all inclusive/blanket concept, then one should not complain about trivialized conclusions to the effect that “everything funds terrorism” and “all channels are used for fund transfers”. Such conclusions would not be particularly helpful to strategic planning, prioritization and focus of limited resources.

For example, as each group uses whatever means are available and each group has different needs and requirements, all kinds of sources will be considered. Then lone wolves (e.g., the two persons who attempted to use a suitcase bomb in Germany in the summer of 2006) will be confused with movements which enjoy popular support and require significant amounts for welfare funding and alternative government functions (e.g., Hamas, the Liberation Tigers of Tamil Eelam [LTTE], Algerian independence movement, etc.).

In another example, one can conceive of a charitable organization where 99.9 percent of its proceeds go as publicly declared, but a tiny fraction may be diverted to support a designated terrorist group. In such case, a blanket concept of terrorism may be accompanied by indiscriminate targeting of the entire charitable organization as well as affiliated financial or other individuals and institutions.

In this report, the discussion is more generic and seeks to offer a general overview of several methods and approaches to financial support and control of groups and organizations officially described as terrorists by many countries and/or the UN and EU. For future purposes, it makes policy and analytical sense to identify and focus on the particular priorities and groups one is concerned about. This will facilitate the setting of concrete targets and objectives, rendering assessments of success or failures more feasible and helpful.

## **Understandings and Definitions of Terrorist Finance**

The United Nations 1999 International Convention for the Suppression of the Financing of Terrorism provides that one commits the offense of terrorist financing if one “by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out an act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex” (nine of the universal instruments against terrorism) or any act “intended to

cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act" (Article 2).

This means that it is not necessary that the terrorist acts are eventually perpetrated or that the funds raised for that purpose were indeed used for these acts. The term "funds" covers "assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit" (Article 1)<sup>8</sup>.

United Nations Security Council Resolution 1373 defines terrorist finance as "the willful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts."<sup>9</sup>

Model international legislative provisions for domestic application in common and civil law jurisdictions have been furnished by the United Nations. The common law draft deals with the provision or collection of property or making available property or financial or other related services directly or indirectly with the intent, knowledge or reasonable belief they will be used toward carrying out terrorist acts in whole or part. Notably, making property or services available is also an offense, if it merely benefits a terrorist group.<sup>10</sup> The civil law version focuses on "An act by any person who by any means, directly or indirectly, willfully provides or collects funds, or attempts to do so, with the intention that they should be used or in the knowledge that they are to be used in full or in part

- a) to carry out a terrorist act, or
- b) by a terrorist, or
- c) by a terrorist organization."

<sup>8</sup> United Nations, International Convention for the Suppression of Terrorist Financing, [http://www.unodc.org/unodc/resolution\\_2000-02-25\\_1.html](http://www.unodc.org/unodc/resolution_2000-02-25_1.html)

<sup>9</sup> United Nations Security Council, Resolution 1373, 28 September 2001, UN Doc. NO. S/RES/1373 (2001). At: <http://daccess-ods.un.org/TMP/7843815.html>.

<sup>10</sup> At: <http://www.imolin.org/imolin/tfbill03.html>.



The text goes on to state that the offense of financing of terrorism “is committed irrespective of any occurrence of a terrorist act referred to in [the previous] paragraph..., or whether the funds have actually been used to commit such act.”<sup>11</sup>

The World Bank and International Monetary Fund offer a most generic definition of the financing of terrorism: “the financial support, in any form, of terrorism or of those who encourage, plan, or engage in it.”<sup>12</sup>

## National provisions

Australia’s law relative to financing a terrorist provides that an offense is committed when one intentionally makes funds available to another person (directly or indirectly); or collects funds for, or on behalf of, another person (whether directly or indirectly); and the first-mentioned person is reckless as to whether the other person will use the funds to facilitate or engage in a terrorist act.<sup>13</sup> The offense is punishable with life imprisonment and committed regardless of the occurrence of a terrorist act, or whether the funds were used to facilitate a particular terrorist act or multiple terrorist acts.

Canada’s arsenal against terrorist finance contains three offenses. The first offense is committed when one “directly or indirectly, wilfully and without lawful justification or excuse, provides or collects property intending that it be used or knowing that it will be used, in whole or in part, in order to carry out” terrorist activity or “any other act or omission intended to cause death or serious bodily harm to a civilian or to any other person not taking an active part in the hostilities in a situation of armed conflict, if the purpose of that act or omission, by its nature or context, is to intimidate the public, or to compel a government or an international organization to do or refrain from doing any act.”<sup>14</sup>

The second offense also requires direct or indirect activity and it relates to the collection or provision, or solicitation to provide property, financial or other services with the intent or knowledge that they will be used in whole or in part, “for the purpose of facilitating or carrying out any terrorist

<sup>11</sup> See Article 5.5 of text available at: [http://www.imolin.org/pdf/imolin\\_ModelLaw-February2007.pdf](http://www.imolin.org/pdf/imolin_ModelLaw-February2007.pdf)

<sup>12</sup> World Bank, & International Monetary Fund. (2006). *Reference guide to anti-money laundering and combating the financing of terrorism* (2nd ed.). [Washington, D.C.]: The World Bank : International Monetary Fund. P I-1. Available at <http://www1.worldbank.org/finance/html/amlcft/referenceguide.htm>.

<sup>13</sup> Anti-Terrorism Act (No. 2) 2005, No. 144, An Act to Amend the Law Relating to Terrorist Acts, and for Other Purposes, 14 December 2005, amending the Criminal Code, 103.2.

<sup>14</sup> Canada, Criminal Code, Part II.1 Terrorism -Financing of Terrorism, R.S.C. 1985, c. C-46, s. 83.02.

activity, or for the purpose of benefiting any person who is facilitating or carrying out such an activity” or with the knowledge that they will be used by or benefit a terrorist group.<sup>15</sup>

The third offense prohibits the direct or indirect use or possession of property with the purpose of facilitating or carrying out a terrorist activity.<sup>16</sup>

Germany has no legal definition of the financing of terrorism and its laws do not provide a separate crime for the financing of terrorism. The financing of terrorism is considered as one possible type of terrorist activity punishable as participation in or support of a terrorist group (see section 129a of criminal code, which does not require the commission of a terrorist act – participation in a terrorist group is sufficient<sup>17</sup>).

Jordan’s law on terrorism finance is limited to the movement of funds within banking/financial institutions, if the funds are related to terrorist activity.<sup>18</sup>

Saudi Arabia, meanwhile, does not define terrorist acts per se, but terrorist financing is handled as a money laundering offense.<sup>19</sup>

Syria’s legislative decree states that the direct or indirect provision or collection of funds, lawfully or unlawfully sourced, for the purpose of a terrorist act, within or outside the country, is a terrorist financing offense.<sup>20</sup>

---

<sup>15</sup> Canada, Criminal Code, Part II.1 Terrorism -Financing of Terrorism, R.S.C. 1985, c. C-46, s. 83.03. This last paragraph s.83.03(b) refers simply to a group’s use or benefit, thereby covering ground beyond the requirements of the 1999 UN Convention, which relates always to a terrorist act. This enables the possible sanctioning of even non-violent activities of a given group.

<sup>16</sup> Canada, Criminal Code, Part II.1 Terrorism -Financing of Terrorism, R.S.C. 1985, c. C-46, s. 83.04.

<sup>17</sup> Interestingly, because the German law’s definition of a “terrorist group” requires three or more persons, the law could not be applied to the 2-person terrorist attempt in the summer of 2006 (when a suitcase with explosives was to be placed in a train; personal interviews). As Dr. Sonja Heine, a German prosecutor, noted in Germany’s 2007 national report to the Association Internationale de Droit Pénal (AIDP) “If the financing of terrorism consists in commerce with a person or organization listed by a UNSC Resolution or the EU this will fall under section 34 of the Foreign Trade and Payments Act (Außenwirtschaftsgesetz). This statute sanctions any activity that provides financial services to or makes available, directly or indirectly, any funds, other financial assets and economic resources to or for a listed person or organization. Penalties vary between 6 months and 5 years imprisonment and a fine and, under aggravated circumstances, between 2 years and 15 years imprisonment. Negligent commission of the offence is also punishable.”

<sup>18</sup> Hashemite Kingdom of Jordan, Penal Code, Chapter Two: Penalty Provisions Related To Time, (3) Terrorism.

<sup>19</sup> Kingdom of Saudi Arabia, The Law of Combating Money Laundering (2003), Royal Decree No. M/39, 25 Jumada II 1421 (23 August 2003).

<sup>20</sup> Syrian Arab Republic, Legislative Decree NO. 22 (2005).

The United Arab Emirates law provides that whoever “gains, provides, collects, carries or transfers property, directly or indirectly, with intention to be used or knows they are going to be used, in whole or in part, to financing any of terrorist acts provided in this Decree by Law within the State or abroad, whether the said act occurred or non occurred,” shall be punished with life or provisional imprisonment.<sup>21</sup> Another article states one who “carries, transfers, deposits property on the account of another person, or conceals or disguises its nature, essence of its source or its place as well whoever possesses property or deal with, directly or indirectly, with intention to be used or knows they are going to be used, in whole or in part, to financing any terrorist acts provided in this Law, within the State or abroad, whether the said act occurred or non occurred,” commits a terrorist act and is subject to imprisonment.”<sup>22</sup> This definition is comparatively more specific than the above two and requires intent and knowledge about an act.

The United Kingdom’s definition specifies that asking another to provide, receiving, or providing money or property with intent or reasonable cause to suspect it may be used for terrorism is an offense. One who possesses such money or property with intent is also guilty as is one who becomes involved in arrangements in which such money or property is made available.<sup>23</sup>

The United States law states that the offense of “material support to terrorists” is committed when someone “provides material support or resources or conceals or disguises the nature, location, source, or ownership of material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out, a violation of” specified statutes<sup>24</sup> or “in preparation for, or in carrying out, the concealment of an escape from the commission of any such violation, or attempts or conspires to do such an act”<sup>25</sup>.

The statute further states that “‘material support or resources’ means any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging,

---

<sup>21</sup> United Arab Emirates, Decree by Federal Law No. 1 of 2004 on Combating Terrorism Offenses, article 12.

<sup>22</sup> Id at article 13.

<sup>23</sup> The United Kingdom, Terrorism Act 2000, Chapter 11, Part III, Terrorist Property.

<sup>24</sup> Specifically, violations of section 32, 37, 81, 175, 229, 351, 831, 842 (m) or (n), 844 (f) or (i), 930 (c), 956, 1114, 1116, 1203, 1361, 1362, 1363, 1366, 1751, 1992, 1993, 2155, 2156, 2280, 2281, 2332, 2332a, 2332b, 2332f, or 2340A of title 18, section 236 of the Atomic Energy Act of 1954 (42 U.S.C. 2284), section 46502 or 60123 (b) of title 49, or any offense listed in section 2332b (g)(5)(B) (except for sections 2339A and 2339B).

<sup>25</sup> United States, 18 USCS, §2339A, Providing Material Support to Terrorists.

training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials.”<sup>26</sup>

It is clear that there is no uniform legal approach to countering the financing of terrorism (CFT). Some jurisdictions mirror UN model laws, while others adopt their own methods or merely extend money laundering provisions to cover CFT. The national regimes vary with respect to the range of activities and groups covered, the types of assets or financial activities included, the origin of funds raised to finance terrorist acts, the intent or knowledge of individuals, whether an activity act or group is financed, etc.

For the present purposes, the general definition of the World Bank and the IMF will be adopted: “the financial support, in any form, of terrorism or of those who encourage, plan, or engage in it”.

### Methods of Fundraising by Terror Groups

Terrorist financing was far from a priority for intelligence collection or academic research before the attacks of 9/11. As a result, research on the topic was thin and based mostly on secondary and superficial sources. The emergence of “instant experts”, who relied on second-hand, sensationalist, biased, out-of-context, and wrong information to make their arguments, has done a disservice to the international community by creating a baseless conventional wisdom that risks misguiding policy and control efforts. Given the spread of “facts by repetition”<sup>27</sup>, we must treat the secondary literature and data with caution and critical spirit, especially in the age of the internet<sup>28</sup>.

The 9/11 Commission criticized early over-enthusiasm about the use of financial controls thus: “But trying to starve the terrorists of money

---

<sup>26</sup> Ibid.

<sup>27</sup> Passas, *Informal Value Transfer Systems and Criminal Organizations: A Study into So-Called Underground Banking Networks* (The Hague: Ministry of Justice, 1999).

<sup>28</sup> For example, a report on the Saudis by French author Jean-Charles Brisard has been self-labeled and cited as a “Report prepared for the President of UN Security Council of the United Nations,” but it was neither solicited nor endorsed by the UN. Jean-Charles Brisard, *Terrorism Financing: Roots and Trends of Saudi Terrorism Financing*, cited in “Saudi Arabia: Terrorist Financing Issues,” Congressional Research Service Reports, 10/03/04, ; available at <<http://fpc.state.gov/fpc/37089.htm>>, accessed 24 June 2005.



is like trying to catch one kind of fish by draining the ocean"<sup>29</sup>. It also demonstrated how wrong statements had permeated policy discussions even with respect to the most investigated case of TF, al Qaeda and the 9/11 hijackers.

At the outset, the Commission frankly admitted, "The nature and extent of al Qaeda fund-raising and money movement make intelligence collection exceedingly difficult, and gaps appear to remain in the intelligence community's understanding of the issue. Because of the complexity and variety of ways to collect and move small amounts of money in a vast worldwide financial system, gathering intelligence on al Qaeda financial flows will remain a hard target for the foreseeable future."<sup>30</sup>

Nevertheless, it has been possible to dispel the popular myth that al Qaeda was drawing on bin Laden's presumed personal fortune from inheritance or businesses he had in the Sudan and elsewhere. It is now clear that particularly after his move from Sudan to Afghanistan, he neither had much personal wealth nor a network of business to rely on<sup>31</sup>.

The 9/11 Commission report detailed the financing of the 9/11 operations and pointed to a number of baseless but persistent media reports and speculation: for example, contrary to media and popular beliefs,

- "there is no evidence the hijackers ever used false Social Security numbers to open any bank accounts"<sup>32</sup>
- "no financial institution filed a Suspicious Activity Report (SAR)... with respect to any transaction of any of 19 hijackers before 9/11"<sup>33</sup>
- "there is no convincing evidence that the Spanish al Qaeda cell, led by Imad Barkat Yarkas and al Qaeda European financier Mohammed Galeb Kalaje Zouaydi, provided any funding to support the 9/11 attacks or the Hamburg participants"<sup>34</sup>

<sup>29</sup> National Commission on Terrorist Attacks upon the United States. 2004. *The 9/11 Commission Report*, National Commission on Terrorist Attacks Upon the United States, Washington D.C. 2004 (subsequently referred to as the 9/11 Commission report), p382.

<sup>30</sup> National Commission on Terrorist Attacks upon the United States. 'Monograph on Terrorist Financing,' Washington, DC: National Commission on Terrorist Attacks upon the United States, 2004, p13.

<sup>31</sup> Ibid. and 9/11 Commission report, p. 20.

<sup>32</sup> 9/11 Commission report, p. 254.

<sup>33</sup> Ibid, p. 545.

<sup>34</sup> Ibid, Chapter 5 footnote 132.

- the Staff monograph on Terrorist Financing has clarified that “Allegations that al Qaeda has used the trade in conflict diamonds to fund itself similarly have not been substantiated”<sup>35</sup> and
- “contrary to some public reports, we have not seen substantial evidence that al Qaeda shares a fund-raising infrastructure in the United States with Hamas, Hezbollah, or Palestinian Islamic Jihad”<sup>36</sup>.

The Staff Monograph also dispelled other popular myths, including the nexus between Barakaat and al Qaeda as well as the theory that al Qaeda profited from short-selling airline shares in the stock market before the 9/11 attacks.

This report will illustrate how wrong assumptions lead to ill-conceived measures, which are both ineffective and counter-productive but first it is important to examine some general aspects of terrorist finance (TF). On an abstract level, the TF cycle may include fund raising, storing, transfer and application or use. The activities most visible, albeit not always identifiable in advance as related to terrorism, are the fund raising and transfers on which we will focus.

A comprehensive description and analysis of the financial aspects of all kinds of terrorism is beyond the scope of this report. It is possible, however, to outline the main elements of fund raising and fund transfers. At the same time, commentary will be offered on items researched in depth on the basis of primary data.

One aspect of terrorist finance is clear and undisputed: there is a wide range of fund-raising methods and sources, some of which are particular to specific groups or contexts, while others are quite common across the board. Some of the funding sources are legitimate, such as ordinary income, legal businesses, investments, charitable organizations and cultural activities. Others sources are criminal, including petty crime, kidnapping, and criminal enterprises of various types. The discussion

---

<sup>35</sup> National Commission on Terrorist Attacks upon the United States. “Monograph on Terrorist Financing.” Washington, DC: National Commission on Terrorist Attacks upon the United States, 2004, p.23.

<sup>36</sup> Ibid, p. 27.

will proceed by examining state sponsorship, illegal and legal sources in sequence, before turning to the fund transfer methods.

### **Legitimate Sources of Funding State Support**

The significance and role of all of funding sources changed substantially at the end of the Cold War, as this signaled a marked decline in state sponsorship of terrorist acts. During the Cold War the major powers funded and supported militant groups and "death squads" in various parts of the globe under the guise of "counter-insurgency" or "international solidarity". Apart from widely discussed examples of politics and diplomacy by other means engaged in by France, USA, or the USSR, several smaller States made their own contributions to bloody conflicts and terrorists. Afghanistan, Cuba, Iran, Iraq, Libya, North Korea, Pakistan, Saudi Arabia, Syria, and Turkey have been among the usual suspects at different periods of time<sup>37</sup>, while many States in all continents have been accused of employing state terrorism themselves in the territories under their control, as they confronted insurgency, rebel or other radical groups.

Well known cases from the past include the state support for extremist Irish, Palestinian, Central and South American, Angolan, South African and other groups. It is worth noting that state sponsorship does not always mean direct (albeit covert) funding; it may also entail the turning of blind eyes to both legal and criminal fund raising activities (e.g., allowing the diversion of charity funds or the operation of arms or drugs trafficking enterprises from which extremist groups benefit). This point is important as it makes clear that the resort to criminal fundraising methods is nothing new. It does not result from less state involvement in terrorism.

Even though virtually everyone agrees that state sponsorship is in decline, the phenomenon has not disappeared. A long list of groups many countries regard as terrorist or subversive are currently supported by states, including Hamas, Hezbollah, Hizbul Mujahideen, the Islamic Militant Union (IMU), Islamic Jihad, Lashkar e Taiba (LeT), Jaish-e-Mohammad (JeM) and Sipah-e-Sahiba (SSP). At the same time, there are

---

<sup>37</sup> See State Department global terrorism annual reports at [www.state.gov/s/ct/rls/pgtrpt/2003/](http://www.state.gov/s/ct/rls/pgtrpt/2003/); Waselar unpublished paper.

glaring examples of continuing state and corporate complicity in atrocities committed by armed militias and other similar organized groups<sup>38</sup>.

The recent decline in sponsorship by major world powers did not make all groups disappear or turn to conventional politics<sup>39</sup>. To the extent conflicts continued, the decline in state sponsorship meant that needs would have to be met through other means. Theoretically, one option was to commit the type of crimes usually committed by actors motivated by profit, while another was to partner with criminal entrepreneurs. Some cross-group support has also been reported suggesting that we ought to keep an eye on how extremist groups may collaborate and support each other<sup>40</sup>. Yet another option is to seek the support of sympathizers.

### **The Ethnic Community and Wider Society: Charities, Businesses, Individuals**

When the issue of charities is raised in the context of terrorism in recent times, most frequently the discussion turns to Islamist terrorism and zakat. Yet, almost invariably, ethnic communities and wealthy supporters have made contributions to parties in conflict back home – for one or the other side. In virtually every conflict, ethnic communities, members, outside supporters and wealthy sympathizers at home and abroad have contributed to respective causes.<sup>41</sup> This may occur through informal revolutionary taxes levied on businesses or entire communities or through direct voluntary contributions and the organization of fundraising events, such as speeches and dinners. Informal revolutionary taxes have been applied by the Palestinian Liberation Organization (PLO) when it

<sup>38</sup> As noted recently, Chiquita Brands International, a big fruit company, agreed to pay \$25 million in fines to the US government for making over several years payments of more than \$1.7 million to Colombian terrorist groups (mainly to Autodefensas Unidas de Colombia - AUC - a right-wing paramilitary organization to which Colombian security forces have turned a blind eye, as well as to the leftist FARC and ELN guerrilla groups). Colombian authorities are also looking into charges that the company used one of its ships to smuggle weapons for the UAC (see Evans, M. (2007). 'Para-politics' Goes Bananas. *The Nation* (April 4), <http://www.thenation.com/doc/20070416/evans>).

Another recent example is provided by allegations that USA has been financing warlord/extremist groups in Somalia; see Sanders, Edmund, "U.S. Role in Somalia Questioned: Government Leaders Charge U.S. with Backing Mogadishu Warlords", *Los Angeles Times*, 2006(May 21); Wax, Emily, DeYoung, Karen, "U.S. Secretly Backing Warlords in Somalia", *Washington Post*, 2006(May 17), A01

<sup>39</sup> Indeed, some of them turned against their erstwhile supporters (e.g., mujaheddin groups in Afghanistan).

<sup>40</sup> For example, Jemaah Islamiya with al Qaeda or Kashmir militants receiving funds from other radical Islamic groups.

<sup>41</sup> See Naylor, R. T. (1993). *The Insurgent Economy: Black Market Operations of Guerilla Organizations. Crime, Law and Social Change*, 20, 13-51.



was outlawed, Fuerzas Armadas Revolucionarias de Colombia (FARC), Autodefensas Unidas de Colombia (AUC), Movimiento 19 Abril (M19), ETA, Provisional IRA, Christian Phalange in Lebanon, the LTTE and other groups.

More generally, militants have drawn on their own ethnic or other communities for funding through direct voluntary contributions and charitable organizations or events. Lashkar-e-Toiba (LeT), for example, uses its public rallies, conferences and evening seminars for fund raising from the general public as well as illegal business activities. Members of the Palestinian Islamic Jihad<sup>42</sup> have apparently employed the following methods, inter alia: (a) fund-raising conferences and seminars; (b) inviting militants from outside the United States to speak at such conferences and seminars; (c) sending letters and other documents requesting funds to individuals and countries in the Middle East and elsewhere; (d) utilizing the Internet computer facilities to publish and catalog acts of violence committed by the PIJ, which are then used to solicit funds for the cause.

It appears that ethnic communities, members, outside supporters and wealthy sympathizers at home and abroad have contributed to respective causes in conflict around the world<sup>43</sup> (e.g., the Irish Republican Army [IRA] and the Irish Northern Aid (Noraid), ETA, LTTE, Al Qaeda, Hamas, Jemaah Islamiya, Korean, Armenian, Khalistani, Chechen, and many others). In an example of fund raising that falls between state sponsorship and private contributions, businesspeople in the US were encouraged to support the Contras after the US Congress prevented the US government sponsorship of this group acting against the government of Nicaragua. In some occasions government officials did the introductions between prominent US-based contributors and the Contras<sup>44</sup>. In other instances, member of an ethnic community may seek the removal of their favorite organizations from documents listing terrorist groups and suspected supporters. A recent example of this is the organization of Tamils for Justice operating in the USA and seeking to raise funds for the purpose of de-listing the

<sup>42</sup> See *US v. al-Arian* indictment. It is very important to note, however, that the jury found al Arian not guilty in most charges and he decided to plead guilty to charges on which the jury was hung in order to expedite his release from prison. The case is ongoing, however, as the prosecution has demanded cooperation he unprepared or unable to offer in other cases, so his detention may be prolonged.

<sup>43</sup> See Naylor, R. T. (1993). *The Insurgent Economy: Black Market Operations of Guerilla Organizations. Crime, Law and Social Change*, 20, 13-51

<sup>44</sup> See Bellant, R., & Political Research Associates. (1991). *The Coors Connection: How Coors Family Philanthropy Undermines Democratic Pluralism*. Boston, MA: South End Press; Rosenbaum, D. E. 1987. Contra Donors Cite North's Role, *The New York Times* (May 22), <http://query.nytimes.com/gst/fullpage.html?res=9B0DE0DD1330F1931A15756C15750A961948260&sec=&=&pagewanted=print>.

LTTE (unsurprisingly their website does not disclose the names of officials, managers or supporters - see <http://www.tamilsforjustice.org/>).

With respect to charities, a distinction can be drawn between those that have had their funds unknowingly diverted and those that have been corrupted and act as fronts<sup>45</sup>. In spite of a notable lack of criminal convictions, government agencies, media and other reports have associated the Global Relief Foundation with al Qaeda, the Holy Land Foundation for Relief and Development and the Quranic Literacy Institute with Hamas, the Islamic Concern Project; World and Islam Studies Enterprises; and the Islamic Academy of Florida with the Palestinian Islamic Jihad<sup>46</sup>. Mosques and non-governmental organizations mentioned in the African embassy bombing trial included the Farouq mosque in Brooklyn, the non-governmental organization Help Africa People and the relief agency Mercy International.<sup>47</sup>

The 9/11 Commission reported that prior to the 9/11 attacks, al Qaeda relied on diversions from Islamic charities and financial facilitators who gathered money from witting and unwitting donors, primarily from the Arabian Gulf region.

Finally, but quite importantly for the most resilient and well organized groups, a diversification into legal businesses has been noted. The Abu Nidal Organization, LeT, LTTE, FARC, [Fuerzas Armadas Revolucionarias de Colombia], Hezbollah, the Irish Republican Army (IRA), and Jemaah Islamiya are among groups that have generated funds through legitimate investments and business activities. Therefore, while a large amount of

---

<sup>45</sup> See the 9/11 Commission report; Also see Maurice R. Greenberg, chair, *Terrorist Financing: Report of an Independent Task Force*, (New York: Council on Foreign Relations, 2003); and Matthew A. Levitt, "The Political Economy of Middle East Terrorism," *Middle East Review of International Affairs*, vol. 6, no. 4, 49-65. Levitt M. 2002b. Combating Terrorist Financing, Despite the Saudis. *Policywatch* No 673, available at: <http://64.233.187.104/search?q=cache:BKQyUelGXj4J:washingtoninstitute.org/watch/Policywatch/policywatch2002/673.htm+POLICYWATCH+Combating+Terrorist+Financing,+Despite+the+Saudis+673&hl=en>

<sup>46</sup> Just as this report was about to be printed, however, a conviction was announced in Boston (not for terrorist finance charges but) for conspiring to defraud the United States and concealing information from the U.S. Government, making false statements to the FBI and filing false tax returns on behalf of Care International, Inc. The main matter was about failing to report to the Internal Revenue Service that Care International used some of its tax-exempt donations to publish a newsletter and other writings in favor of jihad and mujahideen overseas (US v. Muntasser et al.; Murphy, S. (2008). 3 Guilty in Case Tying Charity to Militants. *Boston Globe* (January 12), [http://www.boston.com/news/local/articles/2008/001/2012/2003\\_guilty\\_in\\_case\\_tying\\_charity\\_to\\_militants?mode=PF](http://www.boston.com/news/local/articles/2008/001/2012/2003_guilty_in_case_tying_charity_to_militants?mode=PF)).

<sup>47</sup> USA vs. Usama bin Laden Trial Transcripts: Digital transcripts from the Court Reporter's of Office; available at <<http://cryptome.org/usa-v-ubl-dt.htm>>, accessed 24 June 2005.

the funds used to carry out terror operations originate from crime, it is also true that significant amounts are obtained through licit activities as well.

### Illegitimate Sources

For a variety of reasons, ideologically or religiously motivated offenders may have turned to “ordinary” crime more now than in the past. State disinterest on the one hand and crackdowns on non-profit organizations sympathetic to their cause created a possible gap<sup>48</sup>. At the same time, a number of activities in which militant groups engage have been criminalized in several countries, including the recruitment of members, propaganda through the internet and other means, fund raising, harboring members of designated organizations, gathering of information on their behalf, arms procurement, providing means of communication and other logistical support<sup>49</sup>.

It may also be that terrorists recruit more specialized individual criminals into their ranks, so that it is not actually the whole terrorist group that gets more criminalized, but just certain members<sup>50</sup>. Moreover, it may be that a radicalization of criminal offenders inside prisons or in their communities contributes to a shift from ideology-driven to profit-oriented crimes. Finally, the terrorism-crime nexus includes the possibility that terrorist groups or some of their members may evolve into profit seeking enterprises as their socio-economic and political context changes (or the other way round). An illustration of this possibility comes from the Madrid bombings, where many of the perpetrators were radicalized offenders involved in illicit drug trafficking - they bartered drugs to acquire bomb-making materials<sup>51</sup>.

---

<sup>48</sup> Facilitators and local crime are reported to be the main fundraising options for al Qaeda now according to the UN Monitoring Team (2005: para. 65, 94ff). U.N. Monitoring Team. (2005). Second report of the Analytical Support and Sanctions Monitoring Team appointed pursuant to resolution 1526 (2004) concerning Al-Qaida and the Taliban and associated individuals and entities. New York: U.N. Security Council.

<sup>49</sup> Dandurand, Y., & Chin, V. (2004). *Links Between Terrorism and Other Forms of Crime*. Vancouver: Report to Foreign Affairs Canada and The United Nations Office on Drugs and Crime.

<sup>50</sup> Préfontaine, D. C., & Dandurand, Y. (2004). *Terrorism and Organized Crime: Reflections on an Illusive Link and its Implication for Criminal Law Reform*. Paper presented at the International Society for Criminal Law Reform annual meeting.

<sup>51</sup> This is widely reported in open source, but was confirmed through interviews with those who conducted the financial investigation of the Madrid bombings.



Whatever the precise reasons, there is abundant evidence that ordinary crime is very much part of the political economy of extremism: robberies, extortion, kidnapping, hijacking, informal taxation, and blackmail have been employed by most terrorist groups to secure funds. Protection rackets have been associated in the past with the IRA, ETA, Shining Path, the Abu Nidal Organization<sup>52</sup>. Kidnapping is common in all conflicts, including contemporary Iraq, the whole of South and South East Asia, Africa and Latin America (e.g., Iraqi insurgent groups, FARC, Movimiento 19 Abril, AUC, ETA, the IMU, etc.). Members of the Abu Sayyaf Group have also been reported to take hostages within the Philippines and elsewhere, in order to compel a person or government organization to pay ransom as a condition for the release of the persons detained<sup>53</sup>.

Various types of fraud, with differing degrees of scope and complexity, are employed by contemporary terrorist groups. The GIA and the Salafist Group for Prayer and Combat (GSPC) have been reported to use credit card fraud and document forgery schemes. Two men were convicted at the end of 2007 in Germany for supporting al Qaeda; according to the authorities, life insurance policies were taken out for one of the defendants, who intended to commit suicide bombing in Iraq. The attack was to be covered up through a fake car accident in Egypt and his brother would have received the funds as designated beneficiary of the policies<sup>54</sup>. Al Gamaat al Islamiya, al Qaeda, Hezbollah, the Irish Republican Army (IRA), Chechen insurgents and the Liberation Tigers of Tamil Eelam (LTTE) have reportedly engaged in the counterfeiting of both currency and goods. American, European and Australian currencies have all been illegally reproduced. Some examples of the use of counterfeit goods to raise funds include the illegal copying and sale of intellectual property and computer software, the distribution of counterfeit cigarette stamps, and the manufacture and sale of counterfeit clothing, watches, and copyrighted films, music albums and video games. Interpol has linked intellectual property violations with extremist groups in Northern Ireland, Kosovo and North Africa as well as with al Qaeda<sup>55</sup>. With respect

---

<sup>52</sup> Adams, J. (1986). *The Financing of Terror*. London: New English Library; Horgan, J., & Taylor, M. (1999). Playing the 'Green Card' - Financing the Provisional IRA - Part 1. *Terrorism and Political Violence*, 11(2), 1-38.

<sup>53</sup> See indictment US v. Khadafi Abubakar Janjalani et al. US District Court of the District of Columbia, Crim. # 02-068 (JDB).

<sup>54</sup> Pegna, D. (2007). 3 Convicted in Germany of al-Qaida Aid. *Washington Post* (December 5), [http://www.washingtonpost.com/wp-dyn/content/article/2007/12/05/AR2007120500906\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2007/12/05/AR2007120500906_pf.html).

<sup>55</sup> Noble, R. K. (2003). *The Links between Intellectual Property Crime and Terrorist Financing*. Testimony before the Committee on International Relations: Washington, DC: United States House of Representatives.



to counterfeit goods, it should be noted that, as of the beginning of summer 2006, all intensive efforts of US law enforcement had detected no case of intellectual property violation related to terrorism<sup>56</sup>.

It may be noted, however, that on July 12, 2006, two men pleaded guilty to RICO charges and trafficking in contraband tobacco, counterfeit rolling papers and Viagra, money laundering. Some proceeds of these crimes were passed on to Hezbollah. Sixteen additional persons were charged with the same offenses and participating in the criminal enterprise which operated through Lebanon, Canada, China, Brazil, Paraguay and the United States<sup>57</sup>.

In addition, a recent investigation into counterfeiting, drug trafficking and money laundering has also focused on "the possibility that proceeds from the alleged crime rings have gone for years to Lebanon and the militant Islamic group Hezbollah"<sup>58</sup>.

Other types of fraudulent income-generating activities believed to be used by terror networks include trade scams, tax and value added tax (VAT) fraud, insurance fraud and ATM fraud. Hezbollah members reportedly netted millions of dollars after ordering large containers of merchandise from Asian companies and then defaulting on payments. The IRA has practiced subsidy, tax and VAT frauds<sup>59</sup>, while Lashkar-e-Toiba (LeT) has been linked to insurance fraud involving the filing of false stolen vehicle reports. ATM fraud reportedly played a small part in raising funds for the Madrid train bombing. Finally, the LTTE has also been associated with social security, bank, casino, and immigration frauds<sup>60</sup>.

Human smuggling has also been used in Sri Lanka for militant purposes<sup>61</sup>, while about a quarter of 38 countries surveyed observed the link between terrorism and the smuggling of illegal migrants<sup>62</sup>. The KLA, GIA and

---

<sup>56</sup> Personal interviews.

<sup>57</sup> See *American Chronicle*: "Two Men Plead Guilty to Funding Terrorist Group Hezbollah" (emphasis added)

<sup>58</sup> Krikorian, G. (2007). 6 Accused of Selling Counterfeit Clothing. *Los Angeles Times* (November 15).

<sup>59</sup> Passas, N. (1991). *Frauds Affecting the Budget of the European Community*: Report to the Commission of the European Communities.

<sup>60</sup> Personal interviews in August and November 2004 with a leading prosecutor of terrorism cases in France for the last 25 years, J-L. Brouguères, and with officials at the British Terrorist Finance Intelligence Unit corroborate the view that petty and ordinary crime is a primary source of funds for militancy throughout Europe.

<sup>61</sup> Schmid, A. 2003. "Links between terrorist and organized crime networks: emerging patterns and trends" <http://www.iss.co.za/Seminars/terro19sep03/links.pdf>

<sup>62</sup> Dandurand, Y., & Chin, V. (2004). *Links Between Terrorism and Other Forms of Crime*. Vancouver: Report to Foreign Affairs Canada and The United Nations Office on Drugs and Crime

Jemaah Islamiya have also been reported to involve themselves in this type of illicit enterprise.

The trade in various commodities is another large area ripe for exploitation by militants. The nexus between terrorism and illegal drug trafficking is one of them. This nexus is in fact controversial despite persistent media reports that tend to take it for granted. The term “narco-terrorism” may sound merely descriptive, but it is actually a heavily loaded concept. Although some observers in the 1980s used it to refer to some narco-communist conspiracy of sorts and suggested that left-wing insurgencies trafficked illicit drugs in order to purchase arms from the Soviet Union, the drug trade has attracted guerrilla groups of all races, colors, creed and ideological orientations. Indeed, some of the heaviest involvement in this trade has been by right wing paramilitaries and terrorists<sup>63</sup>. The overuse of this term has also resulted in the poor application of policy and a misidentification of the main issues<sup>64</sup>.

According to a survey of 38 countries, about half of them noticed some link between the drug trade and terrorism<sup>65</sup>. As noted by a UN report, “the Taliban are again using opium to suit their interests. Between 1996 and 2000, in Taliban controlled areas 15,000 tons of opium were produced and exported – the regime’s sole source of foreign exchange at that time. In July 2000, the Taliban leader, Mullah Omar, argued that opium was against Islam and banned its cultivation (but not its export). In recent times, Taliban groups have reversed their position once again and started to extract from the drug economy resources for arms, logistics and militia pay<sup>66</sup>. Even though such links are not surprising, it must be impressed that there are very good reasons why any alliances between terrorists and drug traffickers *cannot* last for very long, due to fundamental incompatibilities of objectives and outlook as well as attitudes toward the State. They are fundamentally different actors with incompatible ultimate goals. Militants desire a change of the status quo, whereas criminal enterprises are politically conservative and simply wish to manipulate or partially neutralize political systems and actors (or divert attention to competing illegal entrepreneurs). In addition, to many militant groups, any open association with drug trafficking or other

---

<sup>63</sup> Naylor, R. T. (2002). *Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy*. Ithaca: Cornell University Press.

<sup>64</sup> Dandurand, Y., & Chin, V. (2004). *Links Between Terrorism and Other Forms of Crime*. Vancouver: Report to Foreign Affairs Canada and The United Nations Office on Drugs and Crime

<sup>65</sup> Ibid. See also CRS 2002 Report: A Global Overview of Narcotics-Funded Terrorist and Other Extremist Groups.

<sup>66</sup> United Nations Office of Drugs and Crime. (2007). *Afghanistan Opium Survey 2007*. Vienna: UNODC, p. iv.

serious crimes would be politically damaging and at loggerheads with their ideology or religious beliefs - thereby undermining recruitment, public and material support efforts. The involvement of al Qaeda in the drug trade, both before and after the 9/11 attacks, has been the subject of some controversy, but no evidence of significant links has been produced.

Similar linkages have been reported with tobacco smuggling (e.g., with respect to Hamas, Hizbollah, IRA, PKK) and with the trade in natural resources. For example, there have been reports of oil for arms barter deals between the Armenian militia in Nagorno-Karabakh and the National Congress of the Chechen People<sup>67</sup>. Cassiterite, cobalt, copper, precious stones, gold and other materials have been fuelling conflicts in Africa despite UN sanctions regimes<sup>68</sup>. Timber<sup>69</sup> and precious stones have also been used as fuel for conflict in several parts of the globe. Particularly controversial have been persistent reports of al Qaeda's involvement in the rough diamond trade in West Africa, which have been contradicted by intelligence and law enforcement agencies, scholarly research and investigative committees<sup>70</sup> (see below case study).

Following in-depth research on this issue, the conclusion is that beyond warring parties and insurgents, some terrorist groups or persons associated with them may have engaged in diamonds transactions, the amounts involved do not appear to be substantial, but the sector is vulnerable for future use by militants. The vulnerability seems to be particularly acute with polished stones (rather than the rough diamonds on which most reports have focused), where the value is more certain, one does not have to be an insider to participate and one can much more easily store and hide value or transfer it across borders.

Most importantly, identified vulnerabilities are not specific to diamonds, but apply equally to trade in general. Trade is currently not transparent and represents a significant threat to all efforts countering money laundering, terrorist finance or other financial crime. The threat is not only potential, but we have already observed cases of trade-facilitated money

67 Graduate Institute of International Studies, *Small Arms Survey*, p. 178.

68 For example, reports of United Nations Security Council panels of experts regarding Angola, the DR of Congo, Liberia and Somalia are replete with such references.

69 Global Witness. (2002). *The Logs of War: The Timber Trade and Armed Conflict*. London: Global Witness.

70 Passas, N. (2004). *The Trade in Diamonds: Vulnerabilities for Financial Crime and Terrorist Finance*.

Vienna, VA: FinCEN, US Treasury Department; Passas, N., & Jones, K. (2006). *The Trade in Commodities and Terrorist Financing: Focus on Diamonds*. *European Journal of Criminal Policy and Research*, 12(available at <http://dx.doi.org/10.1007/s10610-006-9006-3>), 1-33; 9/11 Commission Report 2004.



laundering and terrorist finance. For example, two persons pleaded guilty to charges of conspiracy to violate the Racketeer Influenced and Corrupt Organizations Act by engaging in contraband and passing some of the proceeds on to Hizbollah. The goods in question included contraband cigarettes, counterfeit Zig Zag rolling papers and counterfeit Viagra. The criminal enterprise operated from Lebanon, Canada, China, Brazil, Paraguay and the United States<sup>71</sup>. This is just one of several cases illustrating the vulnerability of trade to significant abuse<sup>72</sup>.

Thus, one need only break up intended deals into a series of financial transactions and engage in some commercial transactions, in order to obscure the investigative trail controllers may wish to follow. The creation of such “black holes” is easy, because data on financial and trade transactions are a) not always accurate and b) not matched to ensure that errors and misstatements can be detected. As a result, irregularities, suspicious transactions and blatant abuses go largely unnoticed.

The heated debate on the role of conflict diamonds in the financing of al Qaeda therefore practically diverted attention from more important policy issues and areas of concern in other parts of the precious stones pipeline and other commercial sectors. Consequently, the possibility of substantial amounts raised or transferred undetected or without the authorities’ ability to identify the contracting parties is a cause for serious concern and a matter that requires urgent attention.

It is also important to note that groups other than al Qaeda are possibly benefiting from or taxing the participants in the precious stones trade (e.g., South Lebanese groups, Northern Alliance).

## **Terror-Crime for Profit Typology**

Sorting out the crime for profit-extremism nexus is beyond the scope of this paper, but it is worth suggesting a tentative typology of the possible connections. This typology does not make any empirical assertions, but rather seeks to organize in a meaningful way reported associations. Its main objective is to assist with differentiating the strength, longevity,

---

<sup>71</sup> See *American Chronicle*, July 12, 2006 “Two Men Plead Guilty to Funding Terrorist Group Hezbollah”; emphasis added.

<sup>72</sup> Simpson, G. R., & Faucon, B. (2007). Trade Becomes Route For Money Tied To Terrorism. *Wall Street Journal*(July 2).



intensity and quality of various associations which require diverse policy responses.

- Firstly, militants may provide **protection** for this trade in territories they control; alternatively, this may be characterized as informal **taxation** of the trade (e.g., Shining Path, AUC, FARC, PKK and tobacco into Iraq).
- Secondly, ideology may be merely **camouflage** for a criminal enterprise (some suggestions in that direction have surfaced regarding Northern Alliance groups<sup>73</sup>, as well as KLA, some Nicaragua Contra groups, some members of 17<sup>th</sup> of November).
- Thirdly, a militant group may be involved as **illegal entrepreneurs** in the trade itself (e.g., the Islamic Movement of Uzbekistan – IMU - or Abu Sayyef). A variation of this is when militant organizations divide labor and assign financing and procurement functions to specific individuals or groups who engage in full-time criminal enterprises (there have been recent examples of this with regard to the LTTE)<sup>74</sup>.
- Fourthly, militants and traffickers may be **partners in the illicit trade** (e.g., Irish paramilitaries, PKK).
- Fifthly, it can be that **individual members** of a group occasionally get involved in the trade (e.g., LTTE, IRA and others).
- Sixthly, some **traffickers may sympathize** with a particular cause and make a contribution in the same way that a legitimate businessman might (see counterfeit and smuggling of tobacco cases cited earlier and below).

73 The vulnerability in that part of the world is underscored by the 2005 State Department's International Narcotics Control Strategy Report, which points out that opium poppy production in Afghanistan is on the rise, with the acreage devoted to poppies soaring almost 240 percent in 2003 – more recent estimates are more alarming.

74 The arrest of Tamil Tiger wanted financier and smuggler, Kumaran Pathmanadan, was first reported in Thailand and then denied; see media reports from the Bangkok Post "Top Tamil Tiger arrested in Bangkok" available at <http://www.bangkokpost.com/topstories/topstories.php?id=121507> and BBC's report entitled "Thailand denies arresting KP" available at [http://www.bbc.co.uk/sinhala/news/story/2007/09/070916\\_kp\\_bangkok.shtml](http://www.bbc.co.uk/sinhala/news/story/2007/09/070916_kp_bangkok.shtml)

- Finally, there may be mere **exchange relations** between terrorist groups and criminal enterprises, such as non-militant individuals or groups procuring arms and conflict-useful materiel (for example, arms traffickers selling to FARC).

Such variety of relationships between criminal enterprises and terrorist groups renders clear the unhelpfulness of terms such as 'narco-terrorism': the policy challenges are rather different when a given group receives some support due to unauthorized/hidden participation of a member in profitable crimes from a situation where a group knowingly comes to depend for its survival and growth on benefits from criminal markets. In the latter scenario, economic incentives may favor the continuation of the armed conflict. Criminal markets in other words may become vested interests in the maintenance of existing power arrangements and undermine any efforts at de-escalation<sup>75</sup>.

## Methods of Transfer

Again, one can hardly find a method that has not been used by one group or another to make payments or transfer funds and value. Militant groups have been able to exploit relatively well-regulated financial systems<sup>76</sup> (as did the 9/11 hijackers), poorly regulated formal banking and wire transfer systems, and informal value transfer systems (IVTS), the regulation of which varies from place to place and over time.

## Informal/Unregulated Channels

The term IVTS refers to ways in which value can be transferred either without leaving easily identifiable traces or entirely outside the formal

---

<sup>75</sup> Such perverse effects and counter-intuitive motives have been noted in African regions where actors were seen as not really aiming for an end to conflicts but their continuation – see Cilliers, J., & Dietrich, C. (2000). *Angola's War Economy: the Role of Oil and Diamonds*. Pretoria: Institute for Security Studies.

<sup>76</sup> U.S. Department of the State, "International Narcotics Control Strategy Report," 2003. Available at <http://www.state.gov/g/inl/rls/nrcrpt/2003/vol2/html/29843.htm>

financial system.<sup>77</sup> IVTS include a wide range of channels, ranging from the simple use of couriers to complex trade arrangements and the use of modern technology, most of which have been actually used by terrorist groups in the past. Some of the IVTS identified include the following:

- Hawala
- Hundi
- Black market peso exchange networks
- Fei chien, door-to-door, and other Asian varieties
- Invoice manipulation schemes
- In-kind fund transfers
- Trade diversion schemes
- Courier services and physical transfer methods
- Corresponding banking accounts employed as sophisticated hawala
- Charities
- Gift and money transfer services overseas via special vouchers and internet web sites
- Digital/Internet based transfers
- Stored value, such as pre-paid telephone cards
- Debit and credit cards used by multiple individuals

---

<sup>77</sup> The term was coined in Passas, N. (1999). *Informal Value Transfer Systems and Criminal Organizations: A Study into So-Called Underground Banking Networks*. The Hague: Ministry of Justice (The Netherlands). See also Passas, "Financial Controls of Terrorism and Informal Value Transfer Methods," in *Transnational Organized Crime: Current Developments*, Henk van de Bunt, Dina Siegel, and Damian Zaitch, eds., (Dordrecht: Kluwer, 2003); Passas, "Hawala and Other Informal Value Transfer Systems: How to Regulate Them?" *Journal of Risk Management*, 2003 [vol. 5 and no. 5]: 39–49; Passas, "Informal Value Transfer Systems, Money Laundering and Terrorism," report prepared for the National Institute of Justice and Financial Crimes Enforcement Network, January 2005, available at <http://www.ncjrs.org/pdffiles1/nij/grants/208301.pdf>, accessed 26 June 2005; Passas, "Indicators of Hawala Operations and Criminal Abuse," *Journal of Money Laundering Control*, Vol. 8(2): 168–172; Passas, *Informal Value Transfer Systems and Criminal Activities* (The Hague: WODC (Wetenschappelijk Onderzoek-en Documentatiecentrum), Netherlands Ministry of Justice); Mohammed el Qorchi, Samuel M. Maimbo, and John F. Wilson, "Informal Funds Transfer Systems: An Analysis of the Informal Hawala System," International Monetary Fund, Occasional Paper No. 222, 2003; Rensselaer Lee, "Terrorist Financing: The U.S. and International Response," Congressional Research Service, Doc. Order Code: RL31658 2002; Samuel M. Maimbo, *The Money Exchange Dealers of Kabul: A Study of the Informal Funds Transfer Market in Afghanistan* (Washington: World Bank, 2003); World Bank Working Paper No. 13). See also, Financial Action Task Force (FATF), 2000–2001 Report on Money Laundering Typologies (Paris: Financial Action Task Force, OECD, 2001); FATF, *Combating the Abuse of Alternative Remittance Systems: International Best Practices* (Paris: Financial Action Task Force, OECD, 2003); and Christine Howlett, *Investigation and Control of Money Laundering via Alternative Remittance and Underground Banking Systems* (Sydney: Churchill Fellowship, 2001).

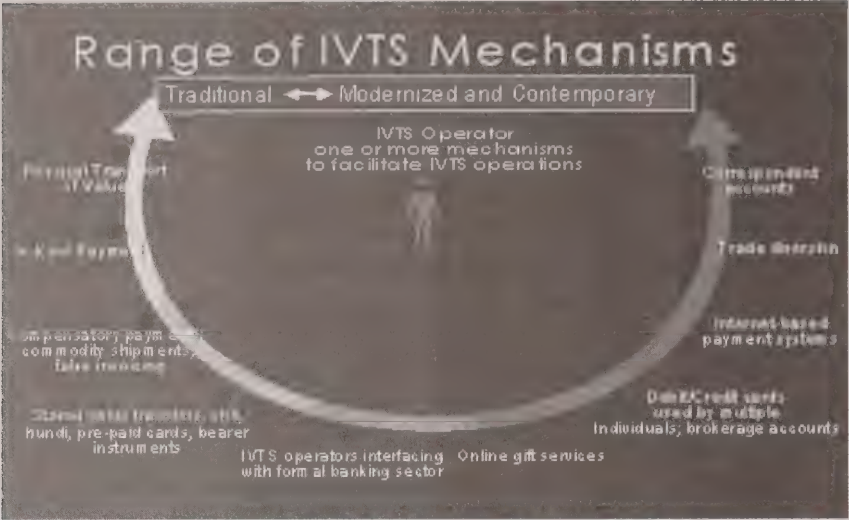


Table 1. Range of IVTS mechanisms from the most traditional to the most sophisticated [networks and single operations may involve more than one method for interim transfers and settlement among the various actors that take part]

Hawala and similar ethnic networks<sup>78</sup> have attracted policy attention and aggressive law enforcement action after the word was uttered during a US Congressional hearing suggesting that this was the preferred method for al Qaeda and similar Islamist groups. Hawala originated in South Asia, possibly centuries ago. The word means “reference” in Hindu (that is, you provide a reference and receive funds or credit in exchange). The Arabic root h-w-l means transfer. Hawaladar is a hawala dealer or operator. Hawala and very similar IVTS operate in many ethnic communities, such as S. Asian, Southeast Asian, Chinese, African, South American and Middle Eastern. It is clearly not a method solely used today by just Muslim communities.

Hawala is a trust-based efficient, convenient and inexpensive method. All it takes is a network of agents and sub-agents who take the remitters’ money, consolidate it, and fax payment instructions to counterparts within the same country or overseas for delivery usually in 24-48 hours

<sup>78</sup> See Passas, “Informal Value Transfer Systems, Money Laundering and Terrorism”; Nikos Passas, 2004. *Informal Value Transfer Systems and Criminal Activities* (The Hague: WODC, Ministry of Justice, The Netherlands). Nikos Passas, *The Trade in Diamonds: Vulnerabilities for Financial Crime and Terrorist Finance* (Vienna, Virginia: FinCEN, U.S. Treasury Department, 2004).



(although this can also be accomplished in minutes in cases of emergency and upon request). Agents balance their accounts through formal and informal channels, sometimes directly and sometimes through a series of third parties.<sup>79</sup> Kashmiri, Hamas, JI, LTTE, and other Asian groups have indeed employed hawala, as have many other organizations, both legal and criminal. Al Qaeda has relied on it when it operated in places where no formal infrastructure or other options were available, especially in Afghanistan. There is no evidence at all, however, that the 9/11 hijackers ever used hawala or similar transfers.<sup>80</sup> In fact, there is only one case so far in the US, Canada or Europe, where Islamist terrorists used hawala for their operations, even though this is an important channel for militants operating in South Asia and Africa<sup>81</sup>.

At the same time, it is important to note that hawala has been used heavily for fund transfers to militant groups in many parts of the world, especially in Asia and Africa, and is vulnerable to abuse by criminals of all sorts, including terrorists. However, even though hawala networks are not transparent in the sense of allowing for easy and accessible review of information/data (instant or automated visibility of transactions related information), they are traceable: access to such information is not instant but there is knowledge of where to go and ask questions about sender, recipient, etc. of transactions (capacity to easily locate and access the relevant information). It is thus important to distinguish between *transparency* (the means of acquiring necessary and useful information) and *traceability* of transactions and counterparties (one of the main goals of financial controls).

Employing physical couriers as a method of fund or value transfer is frequently used for legitimate, criminal and terrorism-related purposes. Whenever formal financial channels are unavailable or too costly, or when

---

<sup>79</sup> The settlement process is vulnerable to abuse and the least visible part of the hawala business. See Passas, N. (2003). Hawala and Other Informal Value Transfer Systems: How to Regulate Them? *Journal of Risk Management*, 5(2), 39-49; Passas, N. (2004). Indicators of Hawala Operations and Criminal Abuse. *Journal of Money Laundering Control*, 8(2), 168-172; Passas, N. (2004). Law Enforcement Challenges in Hawala-related Investigations. *Journal of Financial Crime*, 12(2), 112-119; Passas, N. (2004). Secrets of the Money Trade: Understanding Hawala and its role in the War on Terror. *Northeastern University Magazine*(November), 10-12; Passas, N. (2005). Formalizing the Informal? Problems in the National and International Regulation of Hawala. In *Regulatory Frameworks for Hawala and Other Remittance Systems* (pp. 7-16). Washington, DC: IMF; Passas, N. (2006). Demystifying Hawala: A Look into its Social Organisation and Mechanics. *Journal of Scandinavian Studies in Criminology and Crime Prevention* 7(suppl. 1): 46-62(7(suppl. 1)), 46-62.

<sup>80</sup> See 9/11 Commission Staff Monograph on Terrorism Financing.

<sup>81</sup> This is the case of two persons found guilty in Sweden of "receiving and transferring large sums to the terrorist organization Ansar al-Islam with the aim that the money be used for terror crimes". There are some ongoing cases, in which hawala was allegedly used for the support of terrorist groups.

trust is absent, both legal and criminal actors physically move cash on their own, hand it to friends and relatives or resort to couriers. Cash has been moved in anything from containers to toys, suitcases or even inside one's body. Couriers are also used by money changers in the Middle East, who trade in currencies and therefore need to have the cash in place. Value can also be physically transferred; for instance cash may be used to buy jewelry or gold that can later be sold and its value encashed in the place of destination.

In my own research, I have found that hand carry is occasionally combined with hawala. For example, those wishing to send money to family members in Afghanistan during the Taliban rule had a hard time using hawala channels. As most Afghani families had members residing in Iran or Pakistan, remitters from Europe or the US would use hawala to get the money to relatives in these two countries and ask that they hand-deliver money to their loved ones, when those relatives planned to travel to Afghanistan themselves.

Invoice manipulation. This is an extremely widespread practice facilitative of several types of offenses ranging from tax and duty evasion to capital flight, corruption, money laundering and terrorist finance. One can engage in it by simply mis-declaring the value of exported or imported goods. Under-invoicing sends value secretly, while over-invoicing leads to the receipt of value by the issuer of the invoice.

For example, if goods worth \$100,000 are shipped to Pakistan but the business partner is invoiced for \$150,000, the shipper will receive an additional \$50,000 in North America. Why would a Pakistani importer do this? Because he may wish to minimize his declared profit from the sale of these goods or because he would like the \$50,000 deposited in an account in the US or Europe. So, this can be a method of evading currency and capital controls and of converting funds into a hard currency overseas beyond the government's reach.

Similarly, the value of imports can be understated, so that Customs duties can be evaded or because someone wishes to fund a terrorist operation with the proceeds generated from the sale of higher value imports.

Literally volumes can be written about the vulnerabilities to abuse of trade transactions, which constitute a weak link (possibly the weakest and riskiest link) in AML/CFT efforts and other regulatory regimes (see below section on neglected policy areas).

Charities operating in more than one country have been used to hide the sending of funds to extremists and militants. Small amounts can be diverted from legitimate and needed projects to militants. Raising funds in multiple countries for the same project, for example, may raise no red flags and leave few traces for investigators to follow, unless a global audit of a given group and affiliates is done (more on the charities see below).

Digital/internet-based fund payments can also be used for small amounts that may not trigger any suspicions. Some transactions lending support to the July 2005 bombings in London included international transfers through companies which convert cash into digital currency and allow walk-in clients to remit funds without much due diligence and know-your-customer procedures.

Finally, we have seen the illegal use of correspondent accounts (which are designed and intended for bank-to-bank transactions) to hide illicit transfers for individual clients.

Most observers of terrorist finance suspect that militant groups are moving more towards couriers and hawala methods, partly because of the regulatory and law enforcement scrutiny of the formal banking sector and partly because of their reliability and assumed lower detectability<sup>82</sup>. Hand deliveries through trusted individuals, in particular, are reported to be rising with respect to al Qaeda and many other groups<sup>83</sup>.

## Formal/Regulated Means

The US State Department has argued that terrorist organizations “have exploited poorly regulated banking systems and their built-in impediments to international regulatory and law enforcement cooperation, and have made use of their financial services to originate wire transfers and establish accounts that require minimal or no identification or disclosure of ownership.”<sup>84</sup> Nevertheless, the problems go far beyond some ill-managed institutions or countries with law regulatory regimes.

82 See Lee, R. (2002). *Terrorist Financing: The U.S. and International Response*. Washington, DC: Congressional Research Service. See also U.S. Department of the State, “International Narcotics Control Strategy Report,” 2003. Available at <http://www.state.gov/g/inl/rls/nrcrpt/2003/vol2/html/29843.htm>.

83 See Juan Zarate testimony to Congress; Biersteker, T. J. & Eckert, S. E. (2007). *Countering the Financing of Terrorism*. New York: Routledge. See also Martin A. Weiss, “Terrorist Financing: The 9/11 Commission Recommendation.” CRS Report for Congress. February 2005. At: <http://www.fas.org/sgp/crs/terror/RS21902.pdf>.

84 U.S. Department of State, “International Narcotics Control Strategy Report 2003, n.p.” available at <http://www.state.gov/g/inl/rls/nrcrpt/2003/vol2/html/29843.htm>, accessed 26 June 2005.



For example, the 9/11 Commission report pointed out that al Qaeda funded the hijackers in the United States by three main “unexceptional” means: (1) wire or bank-to-bank transfers from overseas to the United States; (2) hand carrying cash or traveler’s checks into the United States; and (3) debit or credit cards to access funds held in foreign financial institutions. Instead of going through ostensibly weak spots, tax havens, secrecy jurisdictions, or “underground” channels, all of the hijackers used the U.S. banking system, regulated US and British financial institutions, to execute their transactions. Contrary to media and popular belief, the 9/11 Commission report noted that “there is no evidence the hijackers ever used false Social Security numbers to open any bank accounts” and “no financial institution filed a Suspicious Activity Report... with respect to any transaction of any of the 19 hijackers before 9/11”.<sup>85</sup>

So, over \$300,000 passed through the US banking system without triggering suspicious activity reports (SAR) or otherwise raising any red flags<sup>86</sup>. Many observers underlined that funds came through accounts in the UAE, but omitted to add that US and British big institutions were used for the transfers and all amounts ended up in the US in the ‘unremarkable’ ways noted by the 9/11 Commission. For example, Z. Moussaoui brought cash with him, but he duly declared it at the airport raising no suspicions. The 9/11 Commission reported that the hijackers’ transactions should not have triggered suspicious activities reports because compliance officers from the biggest banks have noted the routine nature of the hijackers’ finances. In brief, the argument is that their transactions are similar to the majority of their legal customers. There is no way of differentiating such transactions when used for terrorism and legitimate purposes.

Having seen some credit card statements of 9/11 hijackers, I have some concerns about whether this is entirely accurate and whether some analytical effort could assist both banks and controllers in their work. For instance, the US-based conspirators used credit cards to make cash withdrawals at ATM machines at the maximum limit and routinely in groups of 2-3 individuals at once. This incurred fees and finance charges, which they did not pay at the end of the statement period. They occasionally left all of the balance and did not even pay the minimum amount. Then a deposit would be made in the UAE adding tens of thousands of dollars

---

<sup>85</sup> 9/11 Report, 254 and 545.  
<sup>86</sup> Incidentally, this fact demonstrates that the talk and concerns that followed the 9/11 attacks about the role of low tax and secrecy jurisdictions are off the mark. If there was no such jurisdiction involved in AQ or other terrorist financial scheme, why do we need to raise these as priority problems?



to the credit card account, ending up with a positive balance that would sit there without any interest. Other than cash withdrawals, the credit card was used only rarely for the odd gas station payment or a hair cut. In other words, no living expenses or purchases could be seen in that record. Why would someone have to pay ATM fees using a machine in a shopping mall, when they can use the same card in shops next door instead? This pattern is not a red flag that someone is plotting a terrorist attack, but I am not sure it fits the majority of credit card holders in the US or elsewhere, so it could trigger further inquiries.

In any event, debit and (sometimes pre-paid) credit cards (which can be anonymous and used as a bearer instrument) used by multiple individuals are another alternative to fund transfer. Holders of bank or credit card accounts can have multiple cards on the same account and hand them over to other persons, who use them for withdrawals in other countries. Only the account holder may know, thus, who is taking the cash and for what purpose. However, even she/he may not know where the money and the card goes next, if a terrorist group is reasonably sophisticated, to fragment the division of labor and knowledge of operations.

The Islamic banking system has also attracted policy concerns<sup>87</sup>. Nevertheless, discussions of its actual use are frequently not based on a good understanding of the evidence and operations of Islamic institutions. Before actions are taken, it would make sense to take a number of steps: establish the range of Islamic financial services and instruments available, outline the variations in which they are offered in different countries, analyze the vulnerabilities for abuse (actual and potential) in the future, review existing regulatory arrangements to find out whether such vulnerabilities are addressed, and offer policy recommendations and measures for possible improvements.

Another issue that has generated some debate is the 'storing' of funds by terrorist organizations. As will be seen below, conflict diamonds were reportedly used to store the value of al Qaeda's war chest. Yet, the accounts were later found to be neither founded on evidence nor plausible. In fact, one of the alleged diamond dealers generating and storing millions of dollars has admitted to Guantanamo interrogators that during the entire period when he was supposed to be doing all this in West Africa, he was at an al Qaeda training camp in Afghanistan, which he left after

---

<sup>87</sup> See Landon, T. (2007). Islamic Finance and its Critics. *The New York Times*: August 9). [http://www.nytimes.com/2007/2008/2009/business/2009trust.html?\\_r=2001&oref=slogin&pagewanted=print](http://www.nytimes.com/2007/2008/2009/business/2009trust.html?_r=2001&oref=slogin&pagewanted=print)

9/11 to go to Pakistan (where he was later arrested). The main point to make here is that, again, it depends on what sort of terrorist/militant group we are focusing on. Most threats come in small sizes and budgets. In other words, they would not have any funds to 'store' in any event. Even al Qaeda was operating hand to mouth after they left the Sudan to return to Afghanistan (see amounts involved section below). The matter is different, of course, for groups enjoying wide popular support, having a long history and existence, large membership and governance needs (salaries, health, education, general welfare) when they control territories of a certain size (these were most of the cases discussed by those calling for policy attention to the financing of terrorism as an additional weapon in the counter-terrorism arsenal)<sup>88</sup>.

Given the wide range of raising and transferring funds, it may be useful to make some comments on what general factors may influence the decision of a given militant group to use this or another method:

- Popular support for cause. To the extent a group enjoys legitimacy and sympathy in large sections of a society or population, legal sources of funding are much more likely. The need for criminal methods is diminished. The revelation of shady and illegal sources or practices would have a negative impact on the following and popularity of the group.
- Range/extent of financial needs of a given group
- Size of group. Small militant groups would have limited needs and may be able to accomplish their goals with readily available means. Bigger groups would more likely have to diversify their sources and seek continuous support.
- Scope of activities. One-off, sheer sabotage or bombing activities require fewer resources. On the other hand, if militant activities are only one part of broader political and government-like activities (e.g., security, health-care, education, general welfare, etc.) then very substantial resources will be necessary.

---

<sup>88</sup> Adams, J. (1986). *The Financing of Terror*. London: New English Library.

- Location/Geographic coverage. Fund-raising and transfer opportunities depend on the context in which a group operates. Some areas are rich in natural resources, others lend themselves for illicit drug production, others are close to unguarded borders, still others are in parts of the world with large informal economies and fund transfer methods.
- Ideology/political orientation. To the extent a given group has articulated grievances and an ideological orientation that is incompatible with involvement in certain types of illegal activities (e.g., drug trafficking), the group is likely to stay away from such fund raising methods.
- How well met are the group's needs? Well resourced groups are likely to stay away from illegal enterprises, which attract additional and more international law enforcement attention
- Internal discipline. Some groups may be averse to the use of illegal financing methods or association with criminal enterprises, but the degree to which individual members may get involved in such activities will depend on the strength of the group's internal discipline..

## Amounts Involved

Little is known with certainty and precision about the amount of money involved in terrorist financing and how this is distributed within terrorist organizations. As a result, it is difficult to know whether financial controls targeting large transactions or smaller sums may be more useful and where these controls should be targeted.

There is a serious disconnection between high estimates (popular and repeatedly cited by some presumed experts) and the existing empirical evidence from terrorism cases in N. America and around the world. Some have even spoken of a multi-billion "global economy of terror". Had the reality been even close to such misleading exaggerations, one could consider most current financial controls and other measures in the post 9/11 context at least *prima facie* as reasonable. If the international regulatory net is truly seeking to sweep such gigantic amounts, then the due diligence and reporting processes implemented or recommended

could make sense. Even so, one would be wise to adopt a critical approach, as the overwhelming majority of the measures were a revival and strengthening of AML ideas taken off the shelf and applied to terrorism. Interestingly, such measures were for the most part in the process of being dismantled by US Treasury officials concerned that they would not withstand basic cost-benefit analyses. A growing number of scholars have also voiced serious doubts that the AML regimes have been remotely as successful as AML is officially assumed to be against drug trafficking and other forms of serious criminal enterprises, national and international<sup>89</sup>.

As noted earlier, the problem is that the amounts connected to terrorism are much smaller, despite widespread media as well as 'expert' assumptions to the contrary. For example, if we put together the various theories about al Qaeda's finances, the group would have to be awash with millions of dollars from rough diamonds, gold, charitable donations, legitimate businesses and criminal enterprises including drug trafficking. On the other hand, operatives have been found to be under-resourced or required to raise their own funds for operations. The perpetrators of the first World Trade Center bombing complained that they did not have more than \$19,000 to buy more explosives for a bigger bomb<sup>90</sup>. As al Qaeda departed the Sudan for Afghanistan, many operatives were left behind for they could not afford their modest salaries<sup>91</sup>. Indeed, al Qaeda's wealth has generally been over-estimated. As revealed by computer files retrieved by a reporter in Afghanistan, "The computer did not reveal any links to Iraq or any other deep-pocketed government; *amid the group's penury the members fell to bitter infighting*. The blow against the United States was meant to put an end to the internal rivalries, which are manifest in vitriolic memos between Kabul and cells abroad".<sup>92</sup>

---

<sup>89</sup> See Beare, M. E., & Schneider, S. *Money Laundering in Canada: Chasing Dirty and Dangerous Dollars*. Toronto: University of Toronto Press 2007; Cuellar, M.-F. The Tenuous Relationship Between the Fight Against Money Laundering and the Disruption of Criminal Finance. (2003) *Journal of Criminal Law and Criminology*, 93, 311-465; Naylor, R. T. (1999). Wash-out: A Critique of Follow-the-money Methods in Crime Control Policy. *Crime, Law and Social Change*, 32(1), 1-57; van Dyne, P. C., Groenhuusen, M., & Schudelard, A. A. P. (2005). Balancing Financial Threats and Legal Interests in Money-Laundering Policy. *Crime, Law and Social Change*, 43, 341-377; Reuter, P., & Truman, E. M. (2004). *Chasing Dirty Money: the fight against money laundering*. Washington, DC: Institute for International Economics.

<sup>90</sup> See testimony of Louis J. Freeh, Director, Federal Bureau of Investigation (FBI), "President's Fiscal Year 2000 Budget, before the Senate Committee on Appropriations, Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, Washington, D.C., Feb. 4, 1999 [session of Congress].

<sup>91</sup> See also: "Bin Laden was not entirely devoid of resources on his return. Though his bank accounts were depleted, they still existed and funds from wealthy private backers in the Gulf were still flowing in." (Burke 2004, p. 167)

<sup>92</sup> Cullison, A. (2004). Inside al Qaeda's Hard Drive: Budget Squabbles, Baby Pictures, Office Rivalries—and The Path To 9/11. *The Atlantic Monthly* (September); emphasis added.



So, how much money is currently available to al Qaeda or other groups? The lack of precise answers to this question shows that a more systematic search for information on seizures, estimates of net worth, fund raising capacities, number and type of sympathizers, etc. is necessary. Current estimates, with the notable exception of the 9/11 Commission Report, are often out of touch with the empirical reality as it emerges from trial evidence and investigations.

### **Operating vs. Operational Costs (Acts vs. Large Groups and Infrastructures)**

A proper analysis of the costs of terrorism cannot be done in abstract terms. It is important to differentiate between the funding of particular acts or attacks and the funding for the ongoing operations of an organization or movement. While the cost of an *act* such as a bombing can be trivial, the funding of a militant *group* can involve significant amounts<sup>93</sup>. Such costs would include training, procurement, travel, communications, command and control, propaganda, intelligence gathering and counter-intelligence, bribery of officials, etc. Establishing, maintaining and increasing such *infrastructures*, thus, can be rather expensive. While this is true in general terms, it does not mean that all terrorist groups necessarily require substantial resources. Small and marginal groups may have no expenses at all that cannot be covered by petty crimes or the members' own means and income.

In addition, the operating costs may also relate to legitimate activities. Depending on the longevity, size, targets, methods and objectives of a given group, large *legitimate infrastructures* may also be part of a group's operating expenses<sup>94</sup>. Many insurgent and militant organizations have had extensive welfare, education and social work, security and other functions to perform, especially when they brought limited geographic areas under their control (IRA, LTTE, Hamas, Hizbollah, FARC, etc.). How is one to distinguish between funds needed for terrorism as opposed to the provision of basic services to needy populations? Hezbollah, for example, is said to run twenty-five primary secular schools and has built five

<sup>93</sup> As noted by S. Levey, for instance, "The real operating costs of terrorists inhere in maintaining and perpetuating their networks, and these costs are considerable" (Testimony of Stuart A. Levey, Under Secretary, Terrorism and Financial Intelligence, U.S. Department of the Treasury, before the Senate Committee on Banking, Housing, and Urban Affairs, September 29, 2004)

<sup>94</sup> See Levitt, M. (2006). *Hamas: Politics, Charity, and Terrorism in the Service of Jihad*. New Haven: Yale University Press.

hospitals, with European assistance.<sup>95</sup> Moreover, they cart more than 300 tons of garbage a day from the *dahiyeh*, an impoverished, predominantly Shi'ite area of southern Beirut, and treat it with insecticides.<sup>96</sup> When a decision is made to criminalize a particular organization, such a mixing of militant and legitimate functions, is a moot point, as all relationships with the designated group are prohibited. However, matters are more complicated when the very definition of a given group as terrorist or freedom/independence fighters, insurgents or resistance is in question and leads to diverse approaches in different countries.

Al Qaeda belonged to this category of groups, when it operated out of the Sudan and later in Afghanistan. According to CIA estimates accepted by the 9/11 Commission as reasonable, al Qaeda had a \$30 million annual budget for the overall organization, including \$10-20 million paid to the Taliban<sup>97</sup>.

As Australia's Director of Public Prosecutions suggested in 2003: "al Qaeda spends about 10% of its income on operational costs. The other 90% goes on the cost of administering and maintaining the organization, including the cost of operating training camps and maintaining an international network of cells. So called 'sleepers' must also cost significant sums to establish and maintain"<sup>98</sup>.

The target and context of CFT is very different, when it comes to individual operations, which are mostly quite inexpensive. In many instances, these can be self-financed and low budget. Estimates for the first World Trade Center attack are less than \$19,000, for the Bali bombings less than \$20,000, for the Madrid train bombing about 15,000 € plus the value of some illicit drugs, while a reported attempt at chemical attack in Amman, Jordan that might have caused large numbers of fatalities would have cost about \$170-180,000. The 9/11 operation cost an estimated \$350,000-500,000 over many months (about \$320,000 have been precisely accounted for by the FBI, but some assume that some additional funds were used). As the 9/11 Commission admitted, "The nature and extent of al Qaeda fund-raising and

---

<sup>95</sup> Pasquini, Elaine. 2004. "Hezbollah May Have 'Bright Political Future' in Lebanon, says Dwight J. Simpson." *The Washington Report on Middle East Affairs*. September.

<sup>96</sup> Harik, Judith Palmer. 2004. *Hezbollah - The Changing Face of Terrorism*. New York: I.B. Tauris. Additional services attributed to Hezbollah include surveying for reconstruction projects, preventive spraying for mosquitoes, the provision of drinking water and the expansion of roads; see Sachs, Susan. 2000. "Helping Hand of Hezbollah Emerging in South Lebanon." *The New York Times*. May 30.

<sup>97</sup> 9/11 Commission Staff Report: 27.

<sup>98</sup> Damian Bugg Speech to IAP Conference, December 8, 2003. Available at <http://www.cdpp.gov.au/Media/Speeches/20030812db.aspx>

money movement make intelligence collection exceedingly difficult, and gaps appear to remain in the intelligence community's understanding of the issue. Because of the complexity and variety of ways to collect and move small amounts of money in a vast worldwide financial system, gathering intelligence on al Qaeda financial flows will remain a hard target for the foreseeable future"<sup>99</sup>. In any event, it is not clear, whether al Qaeda in its current form requires or possesses such large amounts of funding or whether the raising and distribution of funds continues to be organized in the same manner as before. Different assumptions of what is or what has become of al Qaeda lead to radically different policy approaches and measures.<sup>100</sup>

---

<sup>99</sup> 9/11 Commission Report, 2004:13.

<sup>100</sup> Contrast, for example, Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror* (New York: Columbia University Press, 2002); and Jason Burke, *Al-Qaeda: Casting a Shadow of Terror* (London : New York: I.B. Tauris, 2003).

At the same time, evidence from terrorism trials and investigations around the world keeps accumulating and reinforcing the impression that terrorism is for the most part inexpensive and that amounts are very often in the thousands if not in the hundreds of dollars (see table below).

<b>Operational Cost of Terror</b>	
•	Madrid 2004 bombings - about 15,000 € (in addition to these operational costs explosives were acquired in a barter deal for illicit drugs with a street value of about 35,000 €)
•	Bali nightclub bombings – about \$20,000
•	US embassy bombings in Kenya and Tanzania – about \$10,000
•	Attacks in Istanbul – less than \$40,000
•	9/11 attacks – about \$320,000 for 19 hijackers over about two years
•	Paris bombs – a few hundred €
•	USS Cole 2000 attack in Aden - less than \$10,000
•	Bishopsgate IRA attack - £3000
•	London 2005 attacks – a few hundred British pounds
•	Jakarta 2003 Marriott Hotel bombing - about \$30,000
•	Chechnya:
•	\$4,000 to down the airplanes;
•	\$7,000 for bomb attacks on Kashirskoye Highway and near metro station.
•	Nord-West operation in Beslan \$ 9,500
•	Germany
•	Planned 2006 train bomb attempt – less than €200
•	Cologne bomb \$241
•	Air India bombings – 3,000 CAD
•	Planned Amman, Jordan chemical attack – \$170,000

Sources: Personal interviews with investigators and prosecutors from the US, UK, France, Germany, Spain, Turkey, FBI; UN Monitoring Team reports; on Jordan: Air Security International; on Chechnya: Shamil Basaev statement; on US East Africa embassy and Bali bombings, 9/11 Commission Staff report: 27-28. It should be noted that an official inquiry into the London bombings in 2005 estimated the total cost of overseas and UK trips, bomb-making equipment, rent, car hire, to less than £ 8,000.



This was funded through defaulted loans, account overdrafts and checks that eventually bounced<sup>101</sup>.

Apart from pointing up the need for collecting all reports on estimates and analyzing them critically, the above suggests that, when it comes to funds for specific operations, we are indeed searching for a needle in a gigantic haystack. The whole infrastructure of financial controls we have put in place against terrorism can assist in undermining, monitoring and investigating terrorist activities, but it is largely irrelevant with respect to finding the relatively insignificant amounts or value that one could carry in a pocket.

While particular acts may be inexpensive, operating costs may be high or low, depending on the terror group in question. In this light, it makes sense to differentiate between the various terror groups.

### **A Typology of Terrorist Groups**

On the one hand, we can have large and popular groups, controlling certain geographic areas and engaged in de facto government functions as well as militant activities (for example, LTTE, Hizbollah, Hamas).

On the other hand, there are small, isolated groups that act independently even though they may be inspired by grievances and arguments voiced by others. Those responsible for the attacks in Madrid, Germany and Glasgow appear to fall under this category.

The second type of groups are unlikely to have extensive financial needs or cross-border transfers and transactions, while the first type will need to raise substantial funds to maintain existing infrastructures and support diverse operations and attacks.

A third type of terror group or network may be placed between the above two ideal types. Small groups acting on their own may also interface with wider networks operating through legitimate ethnic communities, charities and criminal enterprises in several countries. It appears that the group responsible for the attacks in Madrid belongs in this category. A

---

<sup>101</sup> House of Commons, *Report of the Official Account on the Bombings in London on 7<sup>th</sup> July 2005*, HC 1087 11 May 2006. Available at <http://www.official-documents.gov.uk/document/hc0506/hc10/1087/1087.pdf> (accessed April 30, 2007): p. 23.

recent briefing described an apparently self-organizing network in which one finds the Madrid bombers as well as suicide bombers in Iraq and which spreads from Morocco to Spain, other European countries and the Middle East:

- A young person from Mezuak is given the name of someone in Sebta (the Spanish enclave of Ceuta). Money is passed on to handlers connected with, or riding piggyback on, the widespread contraband and drug trafficking that is peculiar to Tetuan and Ceuta (about 25,000 people cross daily from Tetuan into Ceuta without passports).
- Contraband and drug trafficking are integral to Tetuan's economy and even its social fabric, and authorities will not stop it.
- Barcelona is a possible transit point, where there is also a growing Pakistani jihadi community involved in bombing plots in Spain and perhaps elsewhere in Europe. This is a possibility that should be looked into.
- The pipeline seems to resemble the traditional Silk Road that allowed commerce between China and Western Europe for many centuries, where persons at place A would send on merchandise to relatives or other confidants at place B, who in turn would send on or exchange the merchandise to other relatives and confidants at place C, and so on.. Understanding the self generation and maintenance of these networks is a new theoretical challenge for us."<sup>102</sup>

This suggests that between a tiny or marginal group and a large organization with infrastructure, there are networks of support, such as the above. Calculating the cost of suicide bombings in Iraq, thus, would have to consider not only the explosives and intelligence gathering or other preparation for attacks and the travel expenses of a foreigner into Europe, Iraq or other places, but also the general costs of running the

---

<sup>102</sup> Extract from S. Atran and M. Sageman, 2007 "Terror Networks and Sacred Values: Synopsis of report from Madrid – Morocco – Hamburg – Palestine – Israel – Syria"; delivered to NSC staff, White House, Wednesday, March 28, 2007, by Scott Atran, Robert Axelrod and Richard Davis, available at: [http://www.sitemaker.umich.edu/satran/files/synopsis\\_atran-sageman\\_nsc\\_brief\\_28\\_march\\_2007.pdf](http://www.sitemaker.umich.edu/satran/files/synopsis_atran-sageman_nsc_brief_28_march_2007.pdf)

network procuring suicide bombers. In this case, we see an interface with contraband and drug trafficking.

### **Problems with Imperfect Knowledge**

No one would disagree with the principle that counter-terrorism policy and priorities ought to be set in as objective a manner as possible on the basis of good evidence and sound analysis. Because everything has been used to fund one terrorist activity or another, however, special interest groups focused on particular problems seek to associate their cause with terrorism in order to gain support. Occasionally, a consequence of their good intentions and strong commitment to possibly worthy causes is that they divert attention and resources to areas of lower risk or priorities. The same applies to governments seeking external support for the suppression of their political opponents at home, by alleging connections between local groups and al Qaeda.

It could be potentially quite damaging to let priorities set themselves thanks to the differential persuasive or other power of particular groups acting against illicit drug use, counterfeit products, a particular terror group that may not pose as strong a threat (or any) to a given country's national interests. For example, allying ourselves too readily with Central Asian republic authoritarian governments against groups, such as Hizb-ut-Tahrir<sup>103</sup>, can have the effect of radicalizing that group and creating a fertile ground for recruiting more militant and violent actors (e.g., by the IMU).

Three examples taken from the trade in commodities, fund transfers and charities illustrate how exaggerated claims or assumptions not based on solid evidence have led to ineffective and counterproductive measures and policies.

### **“Conflict Diamonds” and al Qaeda: A Theory with no Empirical Support**

Reports that al Qaeda is involved in the trade of conflict diamonds in West Africa have been repeated since 2001. At first, they made a very useful contribution by drawing attention to problems in the regulation of trade in precious commodities as well as to the role of natural resources

---

<sup>103</sup> See Rashid, A. (2002). *Jihad: The Rise of Militant Islam in Central Asia*. New Haven: Yale University Press.

in local or regional conflicts. Subsequently, however, as evidence of al Qaeda fund-raising and value storage in conflict diamonds turned out to be very weak, the reporting of such links continued unabated causing diversion of law enforcement and policy resources away from areas of higher terrorism finance risk areas a) within the diamond sector, b) in other geographic locations and c) other commodities and trade in general.

Media articles indicated that al Qaeda associates have been involved in the conflict diamonds trade, particularly rough diamonds from Sierra Leone mined by the Revolutionary United Front (RUF). It was reported that al Qaeda raised funds through African conflict diamonds and then sought to store value and convert cash into portable, valuable and easily convertible commodities, such as diamonds and gold.

This reporting has been challenged by intelligence and law enforcement agencies, scholarly research and the 9/11 Commission report.<sup>104</sup> While there is cause for concern that the diamond industry can be used to support conflict, terrorist activity and a variety of other crimes, the argument that al Qaeda has had a significant involvement in West African conflict diamonds is unsubstantiated. The al Qaeda-diamonds nexus theory sprang from five main sources,<sup>105</sup> all of which routinely refer to each other and rely on the same or similar material or informants. Careful scrutiny of the quality and consistency of information has belied the allegation that precious stones constituted a significant fund raising or value storage method for al Qaeda.

---

<sup>104</sup> Passas 2004, *The Trade in Diamonds: Vulnerabilities for Financial Crime and Terrorist Finance* (Vienna, Virginia: FinCEN, U.S. Treasury Department). 9/11 Commission report (2004). The Staff Monograph clarifies that "Allegations that al Qaeda has used the trade in conflict diamonds to fund itself similarly have not been substantiated." Staff Monograph, p. 23.

<sup>105</sup> See Doug Farah's series of articles in the *Washington Post*: "Al Qaeda Cash Ties to Diamond Trade," 2 November 2001, p. A01; "Digging Up Congo's Dirty Gems," 30 December 2001, p. A01; "Al Qaeda's Road Paved With Gold; Secret System Traced Through a Lax System in United Arab Emirates," 17 February 2002, A01; "Report Says Africans Harbored Al Qaeda; Terror Assets Hidden in Gem-Buying Spree," 29 December 2002, A01; "Liberian Is Accused of Harboring Al Qaeda," 15 May 2003, A18; "Al Qaeda's Finances Ample, Say Probers," 14 December 2003; and his book, *Blood From Stones: The Secret Financial Network of Terror*, (New York: Broadway Press, 2004). The other four sources are: *The Wall Street Journal* (Block, Robert. "Liberia Cooperates in Study of Terrorist in Diamond Trade." *The Wall Street Journal*. November 21, 2001, p. A11; Block, Robert. "Spreading Influence: In South Africa, Mounting Evidence of al Qaeda Links --- Officials Cite Smuggling Cases And a Deadly Bombing." *The Wall Street Journal*, December 10, 2002, p. A1; a BBC documentary ("Blood Diamonds," October 21, 2001. At: <http://news.bbc.co.uk/1/hi/programmes/correspondent/1604165.stm>); a report by the non-governmental organization Global Witness ("For a Few Dollars More: How Al Qaeda Moved into the Diamond Trade," April 2003), 1-97; and leaked reports or public statements from the Special Court for Sierra Leone (established by an Agreement between the United Nations and the Government of Sierra Leone pursuant to Security Council resolution 1315 (2000) of August 14, 2000) (e.g., "Liberia's Taylor 'Player in the world of Terror,'" AFP, May 15, 2003; Doug Farah, "Liberian Is Accused of Harboring Al Qaeda." *The Washington Post*, May 15, 2003, p. A18).



My own review of the cited sources, interviews with those directly involved in such investigations, and other primary data disconfirm these links. Some of these sources (e.g., the FBI and Belgian federal police) strongly disagree with the media reports and emphasized that, despite time and resources allocated to this effort, they have failed to find transactions indicating unusual transactions and prices at critical times or to corroborate the important components of the al Qaeda and conflict diamonds theory.<sup>106</sup> The 9/11 Commission, which has taken into account additional non-public data (e.g., from al Qaeda detainees) has also pointed out that there is “no persuasive evidence that al Qaeda funded itself by trading in African conflict diamonds.”<sup>107</sup> A Belgian Parliament inquiry and Canadian intelligence sources came to the same conclusion.<sup>108</sup> A review of the 1998 African U.S. Embassy bombing trial shows that the same people who supposedly raised funds from diamonds, also turned to the trade in animal hides, asphalt, assembly watches, bananas, bicycles, butcher equipment, calculators, camels, canned food, cars and tires, cement, fava beans, fish, gold, hibiscus, honey, gemstones, insecticides, iron, lathing machines, leather, lemons, ostrich eyes, palm oil, peanuts, salt, seeds, sesame, shower pipes, soap, sugar, sunflower, tanzanite, textiles, tractors and tractor parts, wheat, white corn, and wood. One has to wonder why al Qaeda associates would stretch themselves so thin, if they could raise the reported millions of dollars through diamonds. Many details of media reports have thus been disconfirmed and their plausibility questioned<sup>109</sup>.

---

<sup>106</sup> Research efforts of more than three years included interviews with intelligence personnel and investigators from the UN, United States and Europe, NGO officials, reporters, industry participants and academics who studied the diamond industry in the past five years. It included also a review of the transcripts and the evidence from the trial for the West African embassy bombings, literature on the subject, public and confidential reports. This study revealed gaps in the evidence, erroneous statements, exaggerations and implausible assumptions. Whether al Qaeda extensively used the rough diamonds trade in its financial operations is doubtful, if it actually dealt in diamonds at all before the 9/11 attacks (Passas, N. *The Trade in Diamonds: Vulnerabilities for Financial Crime and Terrorist Finance* (Vienna, Virginia: FinCEN, [U.S. Treasury Department]. 2004).

<sup>107</sup> 9/11 Commission, (2004: 171).

<sup>108</sup> Christian Dietrich, 2000; Christian Dietrich (2002). Audition de M. Christian Dietrich, (IPIS), diamond analyst, Paper presented at the Commission d'Enquete Parlementaire, Belgique. AVAILABLE AT <http://www.senat.be/crv/GR/gr-06.html> | Royal Canadian Mounted Police, “Link Between Al Qaeda and the Diamond Industry,” 2004; available at <[http://www.rcmp.ca/crimint/diamond\\_e.htm](http://www.rcmp.ca/crimint/diamond_e.htm)>, accessed 26 June 2005.

<sup>109</sup> For example, one of the reported al Qaeda operatives, Ghailani, was said to have dealt in and generated millions of dollars in Africa in the late 1990s and early 2000s. However, he was subsequently arrested in Pakistan and has confirmed to US authorities at Guantanamo Bay that he moved to Afghanistan in 1998 after the Tanzania embassy bombings, went to al Qaeda's al Farouq training camp and stayed there before he found out he was wanted for assisting in the attacks. He moved to Pakistan after the bombing of the country by the US and coalition (see verbatim transcript of open session combatant status review tribunal hearing for ISN 10012: 11-16).

The value storage part of the theory is also weak. If al Qaeda operatives stored substantial assets in rough diamonds, they would have lost about half of their value, as they supposedly bought at 15-20 percent premium<sup>110</sup> and then saw the price fall another 30 percent after 9/11.<sup>111</sup> In addition, such voluminous activities by newcomers would have been noticed by the Lebanese, Jewish and Indian participants in this market or, indeed, the whole industry. Yet, no one reported anything unusual or suspicious at the time or after the al Qaeda allegations were investigated.

In short, the conclusion is that apart from participants in African conflicts, some terrorist groups or persons associated with them may have engaged in some diamond transactions, although the amounts involved do not appear to be substantial. However, the sector is vulnerable to future use by militants. The vulnerability seems to be particularly acute with polished stones (not just the rough diamonds on which most reports have focused so far). Where the value is more certain, as with polished stones, one does not have to be an insider to participate and one can much more easily store and hide value or transfer it across borders.

The media and NGO reports had the effect of pointing out the unexplained resistance of some US agencies to consider precious stones as one possible or potential fund raising and fund transfer medium of AQ. This point has been made, attention has been directed to this industry, and law enforcement is looking into the vulnerabilities. There is no need to keep recycling the same claims further because it became counterproductive: significant law enforcement and intelligence time and resources were applied in Europe, N. America and Africa when they could have been used more effectively elsewhere.

It is important to note that the identified vulnerabilities are not specific to diamonds, but apply equally to trade in general. Trade is currently not transparent and represents a significant threat to all efforts countering money laundering, terrorist finance or other financial crime. The current relative inattention to commercial transactions results in 'nominee trade', whereby authorities have wrong or insufficient information regarding the importer, exporter, value of goods, as well as their origin and final destination. Given the large volumes and numerous actors involved

---

<sup>110</sup> This also begs the question: Why would one voluntarily lose 15-20 percent of the value he is trying to preserve?

<sup>111</sup> Christian Dietrich and Peter Danssaert, "Antwerp Blamed, Again," IPIS (International Peace Information Service); [Diamondstudies.com](http://diamondstudies.com), November 16, 2001.] Accessed at: <http://ossaily.bravehost.com/antwerpblamedagain.htm>.

in the import/export business, significant value transfers and serious misconduct can be hidden behind them.

There are three global flows one needs to pay attention to in order to control terrorism finance and other crimes: financial, commercial and information flows. While most efforts focus on financial flows and to a certain extent messaging and information flows, the problem is that trade flows are neglected. One need only include some commercial or cash transactions in a series of operations in order to obscure the investigative trail controllers would wish to follow. The creation of such “black holes” is easy since financial, trade and information flows are not fully transparent or traceable and are not matched to make sure that what is declared to authorities is what is actually occurring. As a result, irregularities, suspicious transactions and blatant abuses go largely unnoticed. The heated debate on the role of conflict diamonds in the financing of al Qaeda therefore diverts attention from more important policy issues and challenges. Consequently, the possibility of substantial amounts raised or transferred undetected or without the authorities’ ability to identify the contracting parties is a cause for serious concern and a matter that requires urgent attention.<sup>112</sup>

### **Al Barakaat and Terrorism: Links Never Substantiated**

In many parts of the world, hawala is regulated as a money transfer business. In Somalia, however, regulation is left to private sector initiatives because the state is absent. Nevertheless, Somali networks have been the subject of regulatory attention since the attacks of 9/11. Al Barakaat, in particular, has undergone the most thorough scrutiny of any such network anywhere in the world due to allegations that it was closely associated with bin Laden and supported al Qaeda. Media, government reports, terrorism (presumed) experts and high-level officials continue to this day to repeat the early allegations even though none of them has been proven in any country.

Somalia’s principal export during many years of crises has been human labor. Remittance flows have a particularly significant impact on human

---

<sup>112</sup> See Passas, N. (2006). Setting Global CFT Standards: A Critique and Suggestions. *Journal of Money Laundering Control*, 9(3), 281-292; Passas, N., & Jones, K. (2007). The regulation of Non-Vessel-Operating Common Carriers (NVOCC) and Customs Brokers: Loopholes Big Enough to Fit Container Ships. *Journal of Financial Crime*, 14(1), 84-93; available at <http://www.emeraldinsight.com/Insight/viewContentItem.do?contentType=Article&contentId=1585488>; Passas, *The Trade in Diamonds*.



development options there<sup>113</sup>. Al Barakaat used to be the largest remittance provider before it stood accused of sponsoring and providing logistical support to terrorism. In November 2001, the US government accused al-Barakaat of funneling millions of dollars to Osama bin Laden and his Al Qaeda network<sup>114</sup>. The U.S. Treasury Department claimed that Barakaat had been funneling about \$25 million a year from customer fees to bin Laden's network. On the 7<sup>th</sup> of November 2001, police raided Barakaat offices in five U.S. states, seized their records and froze their assets. Similar actions took place around the world, including the United Arab Emirates (UAE), where al Barakaat was headquartered and where top executives were arrested.

Yet, the only terrorist finance accusations were made by government officials speaking at press conferences<sup>115</sup>. The US President, the Secretary of the US Department of Treasury and other high-level officials publicly and repeatedly announced that al Barakaat and its principals were "financiers of terror", "the money movers, the quartermasters of terror", "a principal source of funding, intelligence and money transfers for bin Laden"<sup>116</sup>, used "pseudonyms and shell companies to disguise their true identities"<sup>117</sup>.

I have conducted research into the charges leveled against Barakaat as well as the extensive and intensive administrative and investigative efforts.

It is true that Barakaat operated in forty countries and in depth investigations got off the ground very quickly. Law enforcement and regulatory authorities had al Barakaat and other hawala networks on their radar screen before the flurry of activity in the immediate aftermath of 9/11. The FBI, Customs (Greenquest), OFAC, FinCEN and other organizations paid very close attention to the case and gathered all

---

<sup>113</sup> UNDP (United Nations Development Programme). (2001). *Human Development Report*. New York: United Nations.

<sup>114</sup> For a detailed discussion of the federal government's actions with respect to Al-Barakaat including the November raids, see Chapter 5 of Staff Monograph on Terrorist Financing (Al-Barakaat Case Study), National Commission on Terrorist Attacks upon the United States (9-11 Commission) (2004). [http://www.9-11commission.gov/staff\\_statements/911\\_TerrFin\\_Ch5.pdf](http://www.9-11commission.gov/staff_statements/911_TerrFin_Ch5.pdf)

<sup>115</sup> President Bush, for example stated: "Acting on *solid and credible evidence*, the Treasury Department of the United States today blocked the U.S. assets of 62 individuals and organizations connected with two terror-supporting financial networks -- the Al Taqua and the Al Barakaat. Their offices have been shut down in four U.S. states. And our G8 partners and other friends, including the United Arab Emirates, have joined us in blocking assets and coordinating enforcement action" (emphasis added); see full statement at <http://www.whitehouse.gov/news/releases/2001/11/20011107-4.html>

<sup>116</sup> Exhibit 6 (statement of Treasury Secretary Paul O'Neil).

<sup>117</sup> Exhibit 8.



computers, paperwork and other evidence available in the US. Overseas counterparts acted swiftly and coordinated with US law enforcement. Massive records became available in an unprecedented fashion, as UAE-based Barakaat officials, including the founder, were taken into custody, while all records and evidence were seized. These actions shut down internationally the most successful Somali company and business model, while devastating those working for it in many countries.

The main question is whether al Barakaat's designation as an organization suspected of supporting terrorism and the drastic actions taken against the entire network and its people around the world were based on compelling evidence. One would expect such an impressive collaborative effort and exhaustive global investigation to yield evidence in support of these measures and of terrorism charges.

More than six years after the first press conference on al Barakaat, there is still not a single indictment or charge related to terrorism in the US or any other country that I could identify. The US-based criminal cases dealt with structuring and unlicensed money transmission charges, but not with terrorism.

Within months of the global sanctions on al Barakaat, countries, officials and observers started raising questions about the strength and quality of evidence that could be produced in court or otherwise. For example, Canada was requested to extradite a Barakaat co-defendant in a case in Massachusetts. After thorough investigation, Canada released the frozen funds and defendant, while announcing through a Justice Department spokesperson that they looked at the case and found no evidence:

"Based on a full and thorough investigation of the information collected in relation to the extradition proceedings, the Government of Canada has concluded that there are no reasonable grounds to believe Mr. Hussein is connected to any terrorist activities. The Government has therefore removed him from the list under Canada's UN regulations."<sup>118</sup>

After hundreds of hours spent by federal agents reviewing records and interviewing witnesses about al-Barakaat in Minneapolis, no charges were filed against al-Barakaat participants, with the exception of charges against one customer for a low-level welfare fraud. The FBI in the end decided to close that investigation.

---

<sup>118</sup> See public announcement on official Justice Canada website: [http://www.justice.gc.ca/en/news.nr/2002/doc\\_30513.html](http://www.justice.gc.ca/en/news.nr/2002/doc_30513.html)

The Barakaat allegations and listing by OFAC, the UN and the European Union came increasingly into question by other governments too. International collaboration in counterterrorism efforts were undermined: law enforcement agencies took action at the request of US authorities, but as there was no evidence to justify these actions, overseas counterparts became more cautious and reluctant to act equally swiftly in the future. The lack of evidence in the Barakaat case had also consequences on how the international community was to go about the listing and sanctioning process through the United Nations. Precipitous and unnecessary action is counterproductive and undermines counter-terrorism. Sweden, for instance, attempted to persuade the UN Security Council to adopt a criminal evidentiary standard before anyone is placed on the sanctions list. If that had gone through, most UN designations could have been removed<sup>119</sup>.

Aggressive efforts by US law enforcement to investigate and prosecute terrorist finance through hawala has yielded no case of al Qaeda terrorism so far. Despite media reports and some official statements that hawala was used by the 9/11 hijackers, the evidence shows that formal banks and financial institutions or cash couriers were used by the hijackers and their overseas facilitators. So, not only Barakaat but no other US-based hawala network has been found to assist bin Laden and al Qaeda in their murderous plans<sup>120</sup>.

Law enforcement, intelligence and regulatory officials in the US and many other countries have confirmed to me in personal interviews the authoritative and conclusive statements made by the 9/11 Commission Staff report on Terrorist Finance<sup>121</sup> before and after the publication of this report. It is worth reiterating some of its main observations, which are based on open sources as well as classified information:

Shortly after 9/11 al-Barakaat's assets were frozen and its books and records were seized in raids around the world, including in the United

---

<sup>119</sup> The proposal was defeated after the US State Department urged "in the strongest terms" all Security Council members to oppose it.

<sup>120</sup> Hawala has been used, of course, by bin Laden in Afghanistan and Pakistan, where everyone is using such networks for their efficiency, convenience and low cost or because there is no other alternative. Hawala has also been used in a case of Ansar-al-Islam financing from Sweden to Northern Iraq in support of the insurgency. Another case currently going through the US courts includes allegations that a Pakistani network of hawala operators provided material support to terrorists.

<sup>121</sup> National Commission on Terrorist Attacks upon the United States. (2004). *Monograph on Terrorist Financing* (Staff Report to the Commission). Washington, DC: National Commission on Terrorist Attacks upon the United States.

States. Subsequent investigation by the FBI, including financial analysis of the books and records of al-Barakaat provided in unprecedented cooperation by the UAE, failed to establish the allegations of a link between al-Barakaat and Alai or Bin Ladin. No criminal case was made against al-Barakaat in the United States for these activities. Although OFAC claims that it met the evidentiary standard for designations, the majority of assets frozen in the United States under executive order (and some assets frozen by other countries under UN resolution) were unfrozen and the money returned after the U.S.-based al-Barakaat money remitters filed a lawsuit challenging the action<sup>122</sup>.

The Staff Report goes on to note that “the intelligence sources for much of the reporting regarding al-Barakaat’s connection to al Qaeda have since been terminated by the relevant agency as intelligence sources, *based on concerns of fabrication*”<sup>123</sup>.

The report also notes counter-productive effects of un-substantiated allegations and unwarranted actions using Barakaat as a case study:

When terrorism charges are not possible, the government has brought non terrorist criminal charges against those suspected of terrorist financing. Such an approach, while perhaps necessary, leaves the government susceptible to accusations of ethnic or religious profiling that can undermine support in the very communities where the government needs it most. Moreover, ethnic or geographic generalizations, *unsupported even by intelligence*, can both divert scarce resources away from the real threats and violate the Constitution. Because prosecuting criminal terrorist fund-raising cases can be difficult and time consuming, the government has at times used administrative orders under the IEEPA to block transactions and freeze assets even against U.S. citizens and entities, as we show in the case studies of the al-Barakaat money remitters and the Chicago charities (in chapters 5 and 6). In some cases, there may be little alternative. But the use of administrative orders with few due process protections, particularly against our own citizens, raises significant civil liberty concerns and risks a substantial backlash. The government ought to exercise great caution in using these powers, as officials who have participated in the process have acknowledged, particularly when the entities and individuals involved have not been convicted of terrorism offenses<sup>124</sup>.

---

<sup>122</sup> Ibid at p. 11.

<sup>123</sup> Ibid Footnote 71; emphasis added.

<sup>124</sup> Ibid at p. 50; emphasis added.



In the urgency to act, actions and decisions were made in less than ideal circumstances. In this context, it is not surprising that errors were made and remedial action would be warranted.

The post-9/11 period at OFAC was “chaos.” The goal set at the policy levels of the White House and Treasury was to conduct a public and aggressive series of designations to show the world community and our allies that the United States was serious about pursuing the financial targets. It entailed a major designation every four weeks, accompanied by derivative designations throughout the month. As a result, Treasury officials acknowledged that some of the evidentiary foundations for the early designations were quite weak. One participant (and an advocate of the designation process generally) stated that “we were so forward leaning we almost fell on our face.”

The rush to designate came primarily from the NSC and gave pause to many in the government. Some believed that the government’s haste in this area, and its preference for IEEPA sanctions, might result in a high level of false designations that would ultimately jeopardize the United States’ ability to persuade other countries to designate groups as terrorist organizations. *Ultimately ... this proved to be the case with the al-Barakaat designations, mainly because they relied on a derivative designation theory, in which no direct proof of culpability was needed.* A range of key countries were notified several days in advance of the planned U.S. designation of the al-Barakaat entities, and were urged to freeze related assets pursuant to the own authorities<sup>125</sup>.

Law enforcement became aware of the absence of evidence as well:

Before the second trip [to the UAE], the agent spearheading the effort for the FBI reviewed the OFAC designation package for al-Barakaat and noticed some discrepancies between it and the evidence obtained on the first UAE trip. His review left him with a number of significant factual questions concerning what he thought to be uncorroborated allegations of al-Barakaat’s ties to al Qaeda and AlAI. For example, the designation package described Jumale as an associate of Usama Bin Ladin from the original Afghanistan jihad, who was expelled from Saudi Arabia and then moved to Sudan, and who currently lives in Kenya. However, the documentation obtained from the first UAE trip, including Jumale’s

---

<sup>125</sup> Ibid at p. 79; emphasis added.



passport, did not support that intelligence. In addition, a number of EBI accounts that had been frozen did not appear, from the records obtained and analyzed, to be associated with al-Barakaat at all. Overall, the agent believed that much of the evidence for al-Barakaat's terrorist ties rested on unsubstantiated and uncorroborated statements of domestic FBI sources. The second U.S. delegation to the UAE enjoyed a level of cooperation similar to that of the first. The UAE Central Bank placed 15 people at the investigative team's beck and call. The UAE government did everything the U.S. team requested, including working all night at times to make copies of documents. Jumale was interviewed by U.S. federal agents twice, the first time for ten hours. The U.S. investigative team interviewed 23 individuals (including Jumale), other top al-Barakaat personnel, its outside accountant, and various UAE banking officials. *They also reviewed approximately 2 million pages of records, including the actual EBI bank records.* To review some records, the U.S. government team worked where the records were maintained: in un-air-conditioned warehouses in the desert, in stifling 135-degree heat. *The agents found that the bank maintained the same kind of records as one would find in the United States and that they were relatively complete, well-organized, and well preserved. In fact, it appeared to the agent that the records extended far into the past...*

The FBI agent who led the second U.S. delegation said diligent investigation in the UAE revealed no "smoking gun" evidence—either testimonial or documentary—showing that al-Barakaat was funding AIAI or al Qaeda. In fact, *the U.S. team could find no direct evidence at all of any real link between al-Barakaat and terrorism of any type. The two major claims, that Bin Ladin was an early investor in al-Barakaat and that al-Barakaat diverted a certain portion of the money through its system to AIAI or al Qaeda, could not be verified.* Jumale and all the al-Barakaat witnesses denied any ties to al Qaeda or AIAI, and none of the financial evidence the investigators examined directly contradicted these claims. Moreover, some of the claims made by the early intelligence, such as the assertion that Jumale and Bin Ladin were in Afghanistan together, proved to be wrong. In additional [sic], it appeared that the volume of money was significantly overstated. *Secretary O'Neill, in his announcement of the al-Barakaat action, had estimated that al-Barakaat had skimmed \$25 million per year and redirected it toward terrorist operations. The agents found that the profits for all of al-Barakaat (from which this money would have to come) totaled only about \$700,000 per year, and could not conclude whether **any** of that money had been skimmed*<sup>126</sup>.

<sup>126</sup> Ibid at pp. 82-83; emphasis added; the emphasis on "any" in the line above is in the original report

The conclusions of these investigations were shared. Thus the unsubstantiated and damaging allegations in official and other public statements should have stopped.

At the conclusion of the trip, the agent spearheading the FBI portion of the trip drafted a memorandum, to be distributed to the UAE officials, describing the conclusion the team had reached:

It has been alleged that the Barakaat Group of Companies were assisting, sponsoring, or providing financial, material, or other services in support of known terrorist organizations. Media and U.S. law enforcement reports have linked al-Barakaat companies and its principle manager, Ahmed Nur Ali Jumale, to Usama bin Ladin and bin Ladin's efforts to fund terrorist activities. *However, this information is generally not firsthand information or it has not been corroborated by documentary or other circumstantial evidence that supports the allegation.* For example, it has been reported that it is common knowledge in the United States-based Somali community that Al Barakaat is a money laundering operation backed by bin Ladin. It has also been reported that bin Ladin provided Mr. Jumale the initial financing to start the Al Barakaat businesses. *At this time, these items of information have not been substantiated through investigative means*<sup>127</sup>.

The Report's clearest statement of intelligence and law enforcement evidence-based understanding is that:

Thus, notwithstanding the unprecedented cooperation by the UAE, significant FBI interviews of the principal players involved in al-Barakaat (including its founder), and complete and unfettered access to al-Barakaat's financial records, the FBI could not substantiate any links between al-Barakaat and terrorism. At this writing, neither the FBI nor OFAC is attempting to continue to investigate this case<sup>128</sup>

Finally, one wonders whether all the collateral damage caused by the swift and early actions produced any positive results with respect to counter-terrorism. Yet, the Report is very clear: "To this day, the Commission staff has uncovered no evidence that closing the al-Barakaat network hurt al Qaeda financially"<sup>129</sup>.

---

<sup>127</sup> Ibid at pp. 83-84; emphasis added by the authors of the 9/11 Staff Report.

<sup>128</sup> Ibid at p. 84.

<sup>129</sup> Ibid at p. 81.

US and other government agencies did all they could in a situation of crisis and emergency in order to respond to the attacks of September 11. It is understandable that all leads would be followed and that some executive decisions would be made before the completion of careful investigations. Al Barakat was sanctioned and closed down in a climate of urgency and pressures.

Thorough, sober, lengthy and costly investigations and intelligence-gathering furnished no compelling evidence that any of the public statements and allegations were based in fact. As a result, it is wise and appropriate for everyone to accept the findings, repair the damage done to counter-terrorism and international cooperation against serious crimes, and avoid compounding the problems by insisting on uncorroborated accusations. The connection between Al Barakaat, al Qaeda, bin Laden and other terrorism has not been established.

Problems I pointed out in a 2006 publication have still not been addressed:

“Despite the lack of evidence and formal charges, the names of the owner and the company in Somalia remain on that and the European Union lists ...”

To add insult to the injuries, the 2004-2005 methodologies report of the FATF produced something one is tempted to call “case laundering”. This report of the international standard-setting organization presents a case that left much to be desired as a good practice to be emulated. Under the title “Typology 6: Regulatory Investigation Detects and Disrupts Terrorist Activity”, we find in a box “Case Example 8” and the following text:

MH and his brother were arrested during a crackdown on Somali ARS outlets operating across the United States. In August of 2000, the ARS operator filed an application with the Massachusetts Division of Banks and Loan Agencies for a licence to receive deposits and to transmit money overseas but was never issued a licence. The investigation found that the *Hussein* brothers wired about USD 2.8 million to an account in the United Arab Emirates between September 2000 and November 2001, even though the brothers knew they were breaking the law by not having a state licence. It has been alleged that the profits *supported terrorism*. MH was convicted in April of 2002 of two counts of illegally transmitting money abroad” (emphasis added).



The “analysis” of this case was that:

This is a case where investigation and prosecution for operating an unlicensed ARS service can be used as a method to disrupt a perceived threat of TF. In some jurisdictions, evidence that an ARS [alternative remittance services] operator is acting illegally is more easily obtained than evidence of the larger offence. Disruption of this kind can prompt the formation of a licensed sector serving migrant groups. Education and outreach programmes can help ARS operators to understand their obligations and can serve as the basis for a future prosecution.

The reason why so much detail has been outlined above is to show that there was no real ground on which to take these actions; the terrorism link has not been substantiated despite tremendous resources, global investigations, plenty of records, unprecedented cooperation among authorities. All it caused was collateral damage and animosity unnecessarily. The risk of using the easiest charge is also that unfairness can result when comparatively minor transgressions receive disproportionate sanctions. Not only was there no terrorism charge in this case, but the name of the defendant is disclosed in this report contrary to the routine FATF practice of sanitizing these examples before they go to print after multiple reviews. How “effective” can be the fight against terrorist finance when we devote significant resources tackling an entity found years earlier to have no links with terrorism?. We have also seen that the problem with the US regulatory regime is not so much lack of understanding of remitters’ obligations, but making these obligations realistic, coherent and consistent with public policy objectives.

This case raises the question of whether and how the “Al Capone strategy” of using the easiest charge available should be used. It is reasonable to apply such tactics when we know that we have the right target. The details quoted here is to show that there was no real ground on which to take these actions in the Barakaat case. The terrorism link has not been substantiated despite substantial resources, global investigations, availability and review of plenty of records, unprecedented cooperation among authorities. All the official actions have caused was collateral damage and animosity unnecessarily. The risk of using the easiest charge is also that unfairness can result when comparatively minor transgressions receive disproportionate sanctions.



Ironically, we saw 9/11 hijackers' funds flow through formal Western institutions and – very sensibly – imposed no adverse consequences on them. We saw no funds flow through al Barakaat and yet we devastated the most successful business of Somalia along with the livelihood of all those working for it<sup>130</sup>. Then, we held out all this as a success. Such practices convey messages and create perceptions that are deeply unhelpful in the fight against terrorism and harm international cooperation against serious crime.”<sup>131</sup>

## Charities and Terrorism: Undercutting Our Own Objectives?

All ethnic groups have supported one or another side of conflicts in the homeland, so there is no doubt that non-profit and charitable organizations are a vehicle of possible terrorist finance that must be scrutinized. As pointed out by the UK Charity Commission, charities may assist designated terrorist groups in several ways, including:

- raise money to fund terrorist groups
- use charities to smuggle people into countries
- use charities or supported schools for recruitment and training
- use charities to spread propaganda
- use charities for money laundering purposes<sup>132</sup>

Unsurprisingly, in the context of post 9/11 CFT, non-governmental organizations and charities not only found themselves in the center of the battleground, but have been targeted sometimes in ways apparently

---

<sup>130</sup> Interestingly, piracy is raising funds for warlords in the current conflicts in Somalia, but the international community has done little to deal with that problem. For instance, in 2004, there were only 2 attacks. Since 15 March 2005, 32 attacks took place off the Somalia coast. They usually hijack the vessel, take it into Somali waters beyond the legal reach of foreign naval vessels and demand substantial ransom. Local militias are behind the pirates, providing them with support and protection. We have little insight into where the funds go, but normally, when the ransom is paid, the crew and vessel are released (Source: ICC International Maritime Bureau, Piracy Reporting Centre). It is also interesting to note that the US government has denied allegations that it is financing terrorist groups in Somalia; see Sanders, Edmund, “U.S. Role in Somalia Questioned: Government Leaders Charge U.S. with Backing Mogadishu Warlords”, Los Angeles Times, 2006(May 21); Wax, Emily, DeYoung, Karen, “U.S. Secretly Backing Warlords in Somalia”, Washington Post, 2006(May 17), A01.

<sup>131</sup> Passas, N. (2006). Fighting Terror with Error: The Counter-productive Regulation of Informal Value Transfers. *Crime, Law and Social Change*, 45(4-5), 315-336.

<sup>132</sup> See UK Charity Commission, Operational Guidance, Charities and Terrorism, OG 96 - 29 August 2007 available online at <http://www.charitycommission.gov.uk/supportingcharities/ogs/g096.asp>

not based on solid evidence and through processes which undermine transparency, human rights, the indispensable work charities provide in some of the most challenging parts of the world, and needlessly alienate ethnic and other communities equally concerned about the threat of terrorism and prepared to genuinely assist authorities to prevent it.

At this point, our knowledge is so incomplete that official statements from leading government agencies in the United Kingdom and Canada, for example, point to diametrically opposite conclusions with respect to the extent to which charities have been supporting terrorist groups. According to the UK Charity Commission, “The involvement of registered charities in the funding or support of terrorist activities is *thankfully an uncommon occurrence* but **any** links between a charity and terrorist activity are totally unacceptable.”<sup>133</sup>

Canadian law enforcement has also been alert and active with regard to charities, but the estimated extent of the problem is seen to be much more significant:

Other types of disruptions that we are tracking are RCMP investigations of Canadian charities, which resulted in three charities being denied charitable status because of their links to terrorist activities or groups. This limits the ability of these organizations to raise funds that may be in support of terrorist activity. The work of the RCMP also resulted in the Canada Revenue Agency conducting forensic audits on two charities to examine links to terrorist activity. If the RCMP is unable to address terrorist financing issues in an appropriate manner, Canadians and our allies would be in an environment of elevated risk. Terrorists and their sympathizers would be able to exploit the enforcement weaknesses to collect funds for their operations. As mentioned above, this program has been implemented and thus reduces the risk. Any perceived inability could also have a negative impact on the economic integrity of the Canadian system. Furthermore, *it is important to note that the majority of terrorist financing involves registered charities.*<sup>134</sup>

The estimated extent of the problem ranges from a “thankfully uncommon occurrence” according to the UK Charity Commission to the “majority of terrorist financing” according to the RCMP. It is possible that each agency

<sup>133</sup> Ibid, paragraph 3; italics emphasis added; bold emphasis in original.

<sup>134</sup> See DPR 2005–2006 Royal Canadian Mounted Police, Section II: Performance Results for Departmental Strategic Outcomes and Strategic Priorities; available online at [http://www.tbs-sct.gc.ca/dpr-rmr/0506/RCMP-GRC/rcmp-grc02\\_e.asp](http://www.tbs-sct.gc.ca/dpr-rmr/0506/RCMP-GRC/rcmp-grc02_e.asp)

focuses on different terrorist groups with different funding sources. However, the ethnic make-up of the two countries is not sufficiently different to explain this discrepancy. The point is that we still have a lot to learn.

If every diaspora group has supported one or the other side of conflict in the homeland (e.g, Irish, Armenian, Tamil, Kashmiri, Muslim, Jewish, Chechen, Kurdish, Greek, Palestinian, Basque, Cuban, S. African, Sikh, etc.) and given the clear need for oversight, the chief question is: have we reached an appropriate balance? Unfortunately, heated debates and controversies abound in this policy arena.

An example of negative publicity and unfounded accusations is provided by the case of the Sewa International. Awaas-South Asia Watch published a report in 2004 alleging that Sewa International funded the Rashtriya Swayamsevak Sangh (RSS - Organisation of National Volunteers), an Indian group accused of extremist actions. The report alleged that funds were raised in the course of a Gujarat Appeal for natural disaster relief efforts, village reconstruction and related work, but were diverted to the RSS. The UK Charity Commission investigated the matter and was satisfied that "the trustees have taken sufficient steps to ensure funds have been applied in accordance with the appeal. In January 2004, Sewa International (UK) arranged for a delegation of 30 people from major donors to visit Gujarat to view the completed rehabilitation projects. The delegates produced a report which confirms they were satisfied that the funds had been spent in accordance with the Gujarat appeal". At the same time, the Charity Commission never received formal audited statements, while "its request for visas to visit India to undertake an inspection visit were refused by the Indian government". So, the outcome of the Inquiry gave a much more nuanced version of reality, as a result of which Sewa was allowed to continue its operations in the UK.

Another controversial case is that of the Holy Land Foundation (HLF), the largest Muslim charity in the USA before it was closed down for alleged support of Hamas. The allegation was not about direct contributions but rather that the HLF distributed funds to zakat committees in ways that supported Hamas and its violent campaign (e.g., support of martyrs' and detainees' families). The defense argued that while the indictment charged that funds went to organizations 'controlled by' or 'acting on behalf of' Hamas, none of these organizations were ever designated and that other non-profit actors had been allowed to partner with these

organizations, including the US Agency for International Development. The result of many years of investigations and a long trial was a not guilty verdict for some charges and a hung jury for the rest. Important to note is that HLF was not the only organization affected by this process, because a rather long list of 'unindicted co-conspirators' was published and made available on the internet.

In another two cases covered in the media last year, US authorities seized a \$17,870 payment from the Swedish Trade Union LO-TCO to an educational project in Liberia in March 2006, and impounded two transactions involving the Norwegian Church Aid (NCA) totaling about \$70,000 in 2003 and 2004. The LO-TCO stated that its money was released to the intended Liberian bank after about two months, but only after its Swedish bank vouched for the union's reputation as an established international nongovernmental organization. In the Norwegian Church Aid case, the first transaction was seized in 2003 and released two years later. The financial director of NCA stated: "The second transaction [intended for a YMCA branch in Burma] was confiscated in 2004 and, even though we have sent in the paperwork OFAC [the Office of Foreign Asset Control] required both by fax and PDF file, we still haven't heard anything. I sent the last reminder in January 2007"<sup>135</sup>.

The US Treasury Department's "voluntary" anti-terrorist financing guidelines issued in 2002 have been found by much of the non-profit sector to be unrealistic, impractical and costly<sup>136</sup>. As a result, they are discouraging international charitable activity at a time when it is greatly needed, as witnessed by the recent tsunami disaster and earthquake catastrophe. Moreover, one set of guidelines for all charities would be ill-conceived and dysfunctional, as it ignores the diversity of organizations and the settings in which they offer the various services.

While some limited work has been done in this field, critics of the current arrangement point to the absence of a single conviction of a charity in

---

<sup>135</sup> Collin, C. (2007). Legitimate Charities Snared in Terror Net. *The Washington Times* (22 September), <http://washingtontimes.com/article/20070922/FOREIGN/109220032/109221003>.

<sup>136</sup> See Guinane, Kay, "Safeguarding Charity in the War on Terror; Anti-Terrorism Financing Measures & Nonprofits," Report from OMB Watch, October 2005; Guinane, Kay, "The USA Patriot Act and Its Impact on Nonprofit Organizations," Report from OMB Watch, available online at [www.ombwatch.org/article/articleview/1803/1/\(category\\_id\)](http://www.ombwatch.org/article/articleview/1803/1/(category_id))



the USA on terrorism charges in the past six years<sup>137</sup>, while assets have been frozen and operations shut down or disrupted around the world<sup>138</sup>.

Ultimately, the problem is that crime control and counter-terrorism objectives are undercut as well: a valuable ally - the initially very supportive ethnic communities familiar with conflicts, cultures, arguments, practices and networks through which terrorists recruit and operate - has been alienated by measures and practices widely perceived as unjustified, arbitrary and discriminatory. This process generates frustration among recipients and donors, contributing to a context in which views are radicalized, blind eyes are turned to extreme actions so that militants can more easily recruit supporters and operatives. Terrorism-fuelling grievances and poverty are thus aggravated. Populations in vulnerable positions and politically unstable environments are neglected or abandoned, in some cases receiving aid and services vital to basic needs or survival from the very radicals counter-terrorism policies aim to eliminate. Loyalties and commitments are thereby shaped in a vicious circle adding to militancy and radicalization. Police agencies also find that recruiting informants in these environments is made harder, riskier and costlier too.

Law enforcement and international cooperation are hampered also by overzealous and premature requests for assistance, conducive to designation of organizations and individuals as suspects of terrorism, asset freezes, arrests and investigations. Similarly to the consequences caused by the Barakaat actions we discussed earlier, once such requests prove to be baseless and erroneous, overseas counterparts feel exposed and become reluctant to assist in subsequent cases. Matters get worse when mistakes are found but not admitted and corrective action to repair some of the damage caused to innocent parties is not taken<sup>139</sup>. This is a "lose-lose" situation in which we find ourselves unnecessarily.

---

137 At the beginning of 2008, there was a conviction in a tax related case, where a Massachusetts charity did not disclose to the IRS that it promoted jihad and supported Islamic militants overseas. The case did not include terrorism finance charges; see *US v. Muntasser et al.*

138 In addition to extensive comment on the Barakaat case, the 9/11 Commission also took interest in actions taken against some charitable organizations (see Staff monograph on terrorist finance). It is also instructive to visit the UK Charity Commission website, where results of its investigations are reported. In the case of Palestinians Relief and Development Fund, known as Interpal - a "Specially Designated Global Terrorist" organization for allegedly supporting Hamas' political or violent militant activities on the basis of a US Presidential decree - the Commission reported that the US Authorities were unable to provide evidence to support allegations made against Interpal within the agreed timescale. As a result, Interpal's bank accounts were subsequently unfrozen and the Inquiry was closed in September 2003 (<http://www.charity-commission.gov.uk/investigations/inquiryreports/interpal.asp>).

139 The mis-handling of al Barakaat discussed earlier is a case in point.

## Regulatory Responses

The responses to terrorism financing have been based essentially on thinking and policies developed in relation to money laundering. Given the urgency of the situation and the need to respond quickly and to reassure the wider public that the situation is under control, it is understandable that policy makers would draw on whatever means and experiences appeared relevant to the problem. As noted earlier, anti-money laundering measures were under critical review and about to be scaled back, but in the circumstances, anything that related to the control of criminal funds had to be mobilized. Resistance to such measures from the public at large or the private sector was minimal in a context where everyone wished to appear patriotic and selfless.

Some advantages of such measures were also that quantitative measures of action and success could be provided: one could cite the numbers of designated suspected terrorists, accounts closed, amounts or assets frozen, the growing number of countries following the lead, etc.

One would expect much more careful consideration to be given to similarities and differences between the laundering of criminal proceeds and the funding of militancy in order to ensure that measures are effective and on target. As information and knowledge about terror threats and groups accumulated, the problem and challenges became clearer. The temptation to pursue such financial controls is that they can be politically useful. For example, one may counter evidence of ineffectiveness with tautologies: if terror attacks are fewer, this means that we are succeeding, so no reason to change the approach. If attacks rise, this means that we need to further strengthen our financial controls.

Yet, financial controls remain largely a supply-side approach to crime problems similar to interdiction of illicit drugs. As with the problem of illicit drugs, supply side controls must be complemented with demand side approaches in order to be successful.

In addition, some of the assumptions underlying current financial controls may be incorrect. The first one is that the global "terror economy" is very large and contains a lot of assets to be frozen and seized. As we have seen, this can be wrong in cases of lethal but tiny and independent groups acting with their own means and capabilities. Not all terror groups need or can raise large amounts for their operations.

Another implicit assumption is that the resources available for terror groups and activities are limited. When claims like “Al Qaeda’s cash flow has been reduced by two thirds” are made<sup>140</sup>, one presumes to know the total cash flow of a group whose leaders are still eluding all government authorities. Moreover, such claims assume that no alternative fund-raising methods can be found, such as ordinary crimes for profit committed by members and sympathizers.

We have already seen clearly how small funds can be sufficient to mount terrorist operations with very significant impact. Claiming, thus, that money is the “lifeblood” of terrorism is misleading and unhelpful for counter-terrorism purposes. Such over-emphasis on financial controls may convey the wrong impression that if we turn this life support off, we can stop terrorism. Supply-side counter-terrorism, however, is doomed to fail. This may work against isolated and marginal individuals or groups with no sympathizers or public following. In such cases, identifying and incapacitating them can solve the problem. Nursing such illusions with respect to al Qaeda or other groups the causes of which (if not their methods) command some popular support diverts attention and policy resources from efforts to address the roots of the problem and to construct long-term de-escalation strategies.

To the extent that grievances remain, funds will always be found or made available to those prepared to use violence. We have seen how wide ranging and accessible fund-raising methods are in different contexts. Keeping the historical, socio-economic, cultural and political context in mind is essential and instrumental to more effective policies.

## Objectives and Risks of CFT Policies

Some criticize terrorism financial controls as useless, while others have lofty expectations from them. The truth is in the middle. Targeting terrorist finance is both worthwhile and necessary. CFT can certainly reduce the possible harm of attacks. Secondly, it serves to monitor militant activities so that preventive actions can be taken. In a field where no margin of error is acceptable, this intelligence gathering function cannot be over-estimated. Thirdly, CFT enables the easier reconstruction of events and the discovery of co-conspirators who can then be prosecuted. Finally,

<sup>140</sup> Bowers, F. (2003). Headway on the Al Qaeda money trail *The Christian Science Monitor*/October 1, 2003, available at <http://www.csmonitor.com/2003/1010/p02s02-usfp.html>

the mere knowledge that financial operations are under scrutiny forces extremists to make tactical changes and engage in communications, which generates additional opportunities for intelligence gathering and monitoring.

At a more operational level, the main CFT objectives are higher transparency (e.g., with respect to operators and clients) and traceability of transactions, deterrence and prevention of abuse of financial systems, prevention terrorist finance (e.g., asset seizures), and the monitoring of militants.

The risks of inadequate or ill-thought CFT measures are that we may

- drive networks and transactions underground, losing the opportunity to monitor, prevent, better understand and design long-term strategies
- cause collateral damage and unnecessary economic disruptions,
- alienate ethnic groups<sup>141</sup>,
- undermine our own legitimacy,
- induce superficial (paper) compliance by various countries or agencies, thereby having an ineffective international CFT regime (i.e., rules and laws may be in place, but they are of little use if they go unenforced)
- neglect of more serious problems (regarding terrorist financial vulnerabilities or other serious crimes),
- produce more grievances and provide more fertile ground for the recruitment of new militants. Moreover, if the root causes of terrorism are ignored, the problems the international community faces will remain in place despite apparent successes: that is, even if designated individuals or

---

<sup>141</sup> This would not be the first time: see Ramraj, V. V. (2006). Counter-Terrorism Policy and Minority Alienation: Some Lessons from Northern Ireland. *Singapore Journal of Legal Studies*, 385-404.



groups are arrested or killed in action, other groups or secular radicalism may follow.

### **Cost-Benefit Analyses?**

No one has calculated the precise costs of the international 'war on terror', which includes actions against Islamist extremism as well as other religious and secular groups. New rules, laws and procedures have increased the role and responsibilities of the private sector. This raises questions of transparency and accountability, but also of monetary cost.

Compliance to the 'regulatory tsunami' of international and regional conventions, rules and recommendations of the last few years is a significant challenge to both governments and private companies around the world. Beside proper implementation and genuine enforcement, compliance for private companies has become quite expensive, even though exact figures cannot be produced (companies aggregate several types of expenses for one, but are disinclined to share such information in public). Cost-benefit analyses are common in many areas of public policy, but no such exercise has been undertaken with regard to financial controls of terrorism. The costs are not only financial. Competition, development, human rights and justice may also be affected by misguided CFT measures. Legitimacy, counter-terrorism and anti-crime objectives are also undercut by some of the measures and the neglect of more serious vulnerabilities. This point can be illustrated by the over-emphasis on remittances and the oversight of trade transactions.

### **Are Certain Areas Over-emphasized or Overlooked?**

Hawala and similar traditional ethnic networks enabling the informal transfer of funds around the globe came to the forefront of policy attention due to fears that these were a main financial instrument used by al Qaeda. The regulation of remittances illustrates well the problem of actions taken on the basis of imperfect knowledge, assumptions that Western approaches to control can apply successfully to traditional and informal networks, and lack of broad consensus on the need and appropriateness of particular rules to a given industry.

## Financial Controls and Remittances

As has been frankly pointed out, some initiatives against terrorist finance at the international level have not had the desired effect. For example, the UN sanctions against the Taliban and al Qaeda have not been effective against bin Laden's followers<sup>142</sup>. The nine special FATF Recommendations against terrorist finance would not have red-flagged any of the hijackers' transactions, even if they had been fully implemented before the 2001 attacks. The designation lists of those suspected of providing support to terrorist organizations in the UN, the European Union and particular countries have grown so long and with so many common names as to offer limited assistance and pose issues of due process<sup>143</sup> and enforceability.

AML measures have been extended and become tools in the control of terrorist finance even though doubts are growing about their effectiveness with respect to the laundering of proceeds of serious crime, especially drug trafficking. The amounts involved in terrorism are tiny in comparison to those produced by serious crimes.

Informal fund transfer systems and hawala in particular were singled out from early on as a crucial target in the policies against al Qaeda. Even though such networks have always catered for legitimate remittance needs of millions of immigrants, they are also able to resist controls throughout the world. The way in which countries address informal value transfer systems has varied<sup>144</sup>. Such diversity is not conducive to international cooperation and pushes informal operators underground.

---

<sup>142</sup> U.N. Monitoring Team. (2005). Second report of the Analytical Support and Sanctions Monitoring Team appointed pursuant to resolution 1526 (2004) concerning Al-Qaida and the Taliban and associated individuals and entities. New York: U.N. Security Council.

<sup>143</sup> See, for example, the opinion of the Advocate General in *Kadi v. Council*, Case C-402/05 P, (January 16, 2008), <http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en>, which is expected to have an impact on the listing regime and process not only in the European Union but quite possibly the United Nations as well. In his August 2006 report, Martin Scheinin, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism dealt with the practice of placing individuals and entities on terrorist lists (see A/61/267, paras. 30-41). He acknowledged "the need for preventive action is an important aspect of the fight against terrorism" and emphasized that certain basic human rights must be respected: (a) precise definitions should be used for placement on lists; (b) reviews after reasonable periods, such as 6 or 12 months, necessary to ensure that sanctions remain temporary and preventive, rather than permanent and akin to criminal punishment; and (c) certain procedural guarantees should be utilized for those placed on lists, including proper notice, the right to judicial review (whether at the national or international level), the right to a remedy if wrongly listed, and the right to humanitarian exemptions.

<sup>144</sup> Know-you-customer, record keeping and reporting standards are very asymmetric. Some countries criminalize all informal remittance operations, others outlaw them, many subject them to registration or licensing rules, while other countries do not regulate them at all.

Even at the domestic level, policies have been uncoordinated and even unrealistic. The US regime, for example, has undermined its own stated objectives<sup>145</sup>. At the federal level, the rules for money service businesses (MSBs)<sup>146</sup> include registration, know-your-customer, record-keeping and reporting duties.

At the state level, most jurisdictions require licensing for MSBs. At this level, the regulatory framework is a patchwork of non-pragmatic provisions. The absence of coordination among states and between state and federal authorities has caused confusion, lack of awareness and understanding of specific requirements. Many states' requirements are designed mainly for formal institutions of a certain size, but apply to small, ethnic and informal remitters as well. Cross-state transactions necessitate compliance with the requirements of all states concerned. As can be seen from the table below, bond, capitalization, and other fees entail unaffordable costs to small enterprises and corner shops serving ethnic communities.

---

<sup>145</sup> This analysis draws heavily on Passas, N. (2006). Fighting Terror with Error: The Counter productive Regulation of Informal Value Transfers. *Crime, Law and Social Change*, 45(4-5), 315-336.

<sup>146</sup> MSBs include money transmitters, check cashers, issuer of traveller's checks, money orders or stored value, sellers or redeemers of traveler's checks, money orders or stored value, currency dealing or exchange. Regularly updated information is available at <http://www.msb.gov/>

State	Net worth	Bond	Fee
California	min \$ 500,000 in equity	Determined by Commissioner	\$ 5,000 plus \$50 per agent
Florida	Min \$100,000 plus \$ 50,000 per location in FL up to \$ 500,000	Set by commission rule – max. \$ 250,000 – up to \$500,000	Appl. \$500+\$50 per agent; ren. \$1000 - \$20,000
New Jersey	(1) min. \$100,000 + \$25,000 per agent in NJ up to \$1,000,000. (2) \$50,000 to \$400,000 for foreign money transmitter	(1) \$100,000 to \$1,000,000 (2) foreign remitters: \$25,000-\$100,000 - commissioner may require up to \$900,000	Appl. \$1,000 Lic.: \$4,000 Biannual fee \$25 to \$5,000
New York	Investments equivalent to outstanding payments	Min. \$ 500,000	\$ 500 annual + \$1,000 investig.
Illinois	\$35,000-\$500,000 depending on number of locations	\$100,000 to \$2,000,000	\$100 Appl. \$100 license \$10 per/l – ren. \$100- \$10 p/l
Pennsylvania	\$500,000	\$1,000,000	Appl. \$ 1,000, renewal \$300
Texas	\$25,000 per location up to \$1,000,000	\$300,000 to \$ 400,000	Appl./lic., invest. and renewal [\$500 licensing + \$2,500 invest.]

Table 1. Source: N. Passas (2006) "Fighting Terror with Error: The Counter-productive Regulation of Informal Value Transfers" in *Crime, Law and Social Change*.

Furthermore, failure to comply with a state licensing requirement is a federal offence, even if the defendant was unaware of it. So, the regulatory environment is extremely harsh for new and small MSBs. Not all those who succeeded in raising the necessary capital and meeting these obligations have been allowed to operate.

Following an Office of the Comptroller of the Currency advisory and certain FDIC (Federal Deposit Insurance Corporation) examiners' practices



the message was conveyed to banks that money service businesses (MSBs) constitute a high risk for money laundering and terrorist finance. Consequently, many banks decided to close or not open accounts for hundreds of legitimate operators throughout the USA. Despite efforts from FinCEN (Financial Crimes Enforcement Network), OCC (Office of the Comptroller of the Currency), FDIC and other agencies to address the banks' concern, including a joint statement explicitly stating that banks are not expected to police other financial institutions, the problem remains in 2006.

As noted earlier, hawala has not been used for the 9/11 operations or detected for al Qaeda transactions in North America or Europe. It has certainly been used by al Qaeda in other continents and by other groups. While the potential is certainly there for the use of such channels for terrorist finance (as it is in the formal sector), evidence and analysis points to other areas which should be regarded as matters of higher priority, including trade transparency.

### **CFT and Trade**

One area of high priority is the import-export business. While much attention is focused on informal remitters and general financial controls, commercial transparency is lacking.

Currently, there are serious gaps in the way government authorities deal with trade transactions. Incomplete, erroneous or illegal documentation can be found through routine review of forms filed with Customs agencies. There is plenty of room for improving enforcement action and attempts at rendering the transactions accurate and transparent. Mistakes and mis-statements concerning country of origin, ultimate consignee, counter-parties or value abound and reveal significant opportunities for misconduct, including terrorist finance. In other instances, trade diversion practices and mis-invoicing cannot be easily detected as the paperwork in such cases is not forged or fake but the content of the documents is wrong. Very high values can be moved literally under the nose of even quite careful inspectors. Such infractions may only be detected through inside information or in-depth checks and inquiries, which cannot be routinely instituted.<sup>147</sup>

---

<sup>147</sup> Due to the trade and financial disruption they would cause.

Such vulnerabilities were found in the trade of precious stones and metals, electronics, medicine, cosmetics, textiles, foodstuff, tobacco, car or bicycle parts, etc.. In short, trade is currently not transparent and represents a serious threat to all efforts countering money laundering, terrorist finance or other financial crime.

Given that financial and trade transactions are not jointly monitored and matched, irregularities, suspicious transactions and blatant abuses may be going undetected. Research has shown that irregularities amounting to billions of US dollars go undetected and uninvestigated<sup>148</sup>. In the light of the large volumes of trade conducted daily, the risk of financing serious crime includes activities not only related to more expensive forms of terrorism as well as proliferation and weapons of mass destruction.

## Policy Implications

In the aftermath of 9/11, national and international measures were introduced with the aim of controlling terrorist finance: identifying supporters and funding sources, tracking and stopping money flows, freezing and confiscating assets. The UN convention for the Suppression of the Financing of Terrorism was speedily ratified and entered into force and UN Security Council Resolutions<sup>149</sup> resulted in national progress reports on the implementation of CFT measures. The Financial Action task Force (FATF) quickly added nine special recommendations on terrorism finance complementing its 40 previous recommendations against money laundering. World Bank and IMF assessment and evaluation practices included terrorist finance. International organizations such as the United Nations and the European Union as well as several countries maintained growing lists of suspected terrorists and supporters. Many countries introduced laws and issued executive orders aiming at assets suspected of belonging to or supporting designated terrorist organizations.

---

<sup>148</sup> Naim, M. (2005). *Illicit: How Smugglers, Traffickers and Copycats are Hijacking the Global Economy*. New York: Doubleday; Passas, N. (2006). *Terrorist Finance and the Nexus with Transnational Organized Crime: Commodities Trade*. Washington D.C.: Report to the National Institute of Justice (NIJ); Passas, N. (2006). Setting Global CFT Standards: A Critique and Suggestions. *Journal of Money Laundering Control*, 9(3), 281-292; Passas, N., & Jones, K. (2006). The Trade in Commodities and Terrorist Financing: Focus on Diamonds. *European Journal of Criminal Policy and Research*, 12(available at <http://dx.doi.org/10.1007/s10610-006-9006-3>), 1-33; Passas, N., & Jones, K. (2007). The regulation of Non-Vessel-Operating Common Carriers (NVOCC) and Customs Brokers: Loopholes Big Enough to Fit Container Ships. *Journal of Financial Crime*, 14(1), 84-93; available at <http://www.emeraldinsight.com/Insight/viewContentItem.do?contentType=Article&contentId=1585488>

<sup>149</sup> See UN Security Council Resolution 1267, which imposed financial sanctions against the Taliban in Afghanistan and established a Committee to monitor and enforce them. After 9/11, UN Security Council Resolution 1373 established procedures to shape CFT measures.

Controlling terrorist finance is vital and necessary. Particularly important are the functions of monitoring, intelligence gathering and prevention that can be performed or facilitated through such controls. Mechanisms put in place against money laundering have been strengthened and supplemented with additional ones, all of which enables the tracing of certain transactions and activities, which is helpful for law enforcement purposes as well.

However, over-emphasis on the supply-side of counter-terrorism leads to a comparative neglect of demand side approaches (e.g., what fuels militancy and the willingness of so many individuals to engage in extreme acts or suicide in the name of a given cause). Short term, military and law enforcement approaches are then not sufficiently supplemented by long-term socio-economic and political strategies. Imperfect knowledge and vested interests left un-scrutinized for analytical quality, objectivity and accuracy have compounded the problem and created a misleading conventional wisdom based on 'facts by repetition'.

Claims of success notwithstanding<sup>150</sup>, the CFT arsenal was developed and applied too fast, to the point of being in several respects unnecessarily costly, ineffective, unfair and even counterproductive. In addition, many of the control functions have been de facto outsourced to the private sector without proper guidance and accountability.

In general, new controls were introduced to enable government authorities to trace the source and destination of various funds and assets, task forces were set up to investigate and prosecute terrorist financing, international cooperation between countries and agencies was encouraged, new laws criminalized the financing of terrorism, know-your-customer and suspicious activity reporting requirements contributed to promoting greater financial transparency, and name-and-shame policies sought to induce compliance.

The success of these controls has been measured occasionally by the amount of money and number of bank accounts that have been frozen, or the number of suspicious activity reports filed by financial institutions.<sup>151</sup>

<sup>150</sup> See, for example the recent views of a former US government official in Jacobson, M. (2008). Extremism's Deep Pockets: The Growing Challenge of Fighting Terrorist Financing. *The Politic.org*, <http://thepolitic.org/content/view/91/37/>.

<sup>151</sup> See 'UK Minister Calls For Less Money Secrecy To Combat Terrorism', *Crime Reporter* 11.0. October 15, 2002 [Address by UK Foreign Office Minister Denis MacShane at the FT Conference in London on 15 October: "Fighting Financial Crime"].



In other instances, the number of prosecutions or closures of unlicensed remitters has been discussed as measure of progress. By such standards, controls over formal and informal financial institutions may be considered successful. Even though it is difficult to determine how many terrorist attacks have been actually thwarted by these actions, it is possible that amounts that could have been used to support militant infrastructures or operations have been taken away.

Over-reliance on these methods, however, may lead to misapplications. As the 9/11 Commission and others have pointed out, in several cases, asset freezing and designations turned out to be premature and problematic. A very large part of the funds and assets that have been frozen are of “suspected” or “alleged” terrorists and supporters. In many cases, there has been no strong evidence to support the arrests, freezing of assets and statements that government officials have made, causing serious damage to innocent parties through processes that afford them no opportunity to challenge their designation and without formal charges leveled against them.

More critically, some of the measures may be not be just ineffective in increasing transparency, traceability and prevention of terrorist finance, but also counter-productive. Instead of promoting transparency and traceability of transactions, the result may be that more actors go underground and employ obscure value transfer methods with which controllers are less familiar. Instead of strengthening alliances against terror, some communities may feel marginalized or alienated. Instead of supporting and collaborating with non-governmental organizations active in conflict zones, we may be undercutting their de-escalation and humanitarian assistance work. Instead of bringing a growing share of economic transactions into formally regulated and well monitored vehicles, we may be pushing more economic activity underground. Instead of enhancing possibilities of intelligence gathering and monitoring of suspect groups, we may be losing opportunities to gain insights into terror groups and planned attacks. Instead of focusing our efforts on the highest risks and threats, we may be leaving the worst vulnerabilities unattended. Instead of contributing to better security, we may end up with more grievances and fertile ground for militant recruitment and extreme actions.

This is where the apparent consensus over the means and objectives of CFT ends and the debates begin on the top priorities and how to address



them. In order to move this debate forward, this report concludes with a discussion of policy implications under three main headings: evidence-based policy making, identification of high-risk areas and trade transparency, and legitimacy.

## **Evidence-Based CFT Policy Construction**

Effective policies against terrorist finance can only be based on solid empirical evidence and analysis. Self-evident as this may appear, we have seen how imperfect knowledge and particular interests or concerns have affected priorities and approaches at the national and international levels. An important task, thus, is to establish the facts on comparative risks (e.g., in particular areas in the formal and informal sectors, finance and commerce, profit and non-profit institutions, etc.). This sort of threat assessment can be conducted through the *systematic* and *comprehensive* collection and review of all available evidence and policy arguments, an endeavor that has still not been undertaken. This involves the following tasks.

### **Establish the Nature and Social Organization of Extremist Groups**

Fighting “terrorism” in general may sound like a worthy cause, but it is unrealistic to expect that all groups so defined can be effectively fought at the same time. There are simply too many terrorisms and extremism around the globe for even the mightiest country to tackle them all at once. It is essential that each country focus on the top risks and threats with the proper balance of urgency and commitment to doing this well and right. Many would agree that al-Qaeda and groups considered as associated with it pose the most serious and imminent risks<sup>152</sup>.

Nevertheless, even on this point we cannot be entirely sure we have correctly identified the main target, for there are divergent views on the nature, social organization and structure of al-Qaeda. Different assumptions of what is or what has become of AQ lead to radically different approaches

---

<sup>152</sup> At times the severity of the threat has varied. For example, a secret FBI report leaked some time ago to the media suggested that their capacity to inflict harm in the US at the time had been drastically reduced and that, contrary to official positions, there were no sleeper cells in the country (Whitaker and Meo, 2005).

and measures<sup>153</sup>. If we believe that al Qaeda is a relatively stable network or that it possesses some elements of a hierarchical organization, then we would expect more predictable flows of information and funds that could be targeted with the current CFT policies based on models used in anti-money laundering (AML) and counter-drug efforts. Interestingly, to the extent that such policies degrade the more stable organizational patterns and network nodes of al Qaeda, such as those that existed in Afghanistan during the Taliban regime, this would tend to contribute to the group's transformation into a loose coalition of small cells held together by a worldview and shared enemies rather than a network—an unintended consequence that would make al Qaeda members harder to identify and attack.

Others have argued that al Qaeda was never such an organization, but an idea or worldview that inspires locally operating individuals and groups. Either way, the point is that at the present time al Qaeda is not the sort of affluent and rationally organized group that conventional wisdom imagines. Bin Laden and his followers do not have big fortunes or huge assets to draw on. Rather, the amount of funds to be controlled appear to be much smaller, while the means used to raise them vary widely, include ordinary crime and depend on local conditions. In this light, there would be less of a need for cross-border fund transfers, while communications among different terror groups or other intelligence we may seek to extract by monitoring such operations would be limited.

Besides al Qaeda, there are many more terrorist threats that different countries can be expected to perceive as of a higher or lower priority. Each of these groups would need to be examined and understood to ensure that the appropriate measures are applied as needed.

## Determine the Size of Funds Available to Extremists

In addition to *theoretical* or analytical arguments on al Qaeda's finances, there is a marked discrepancy between high estimates (popular and repeatedly cited as they are) and the available *empirical* evidence. If we

---

<sup>153</sup> Contrast, for example, Gunaratna, R. (2002). *Inside Al Qaeda: Global Network of Terror*. New York: Columbia University Press with more critical statements by Burke, J. (2003). *Al-Qaeda: Casting a Shadow of Terror*. London and New York: I.B. Tauris or Naylor, R. T. (2006). *Satanic Purses: Money, Myth, and Misinformation in the War on Terror*. Montreal and Kingston: McGill-Queen University Press. See also a more recent and empirically founded assessment of al Qaeda in Sageman, M. (2008). *Leaderless Jihad: Terror Networks in the Twenty-first Century*. Philadelphia: University of Pennsylvania Press.

put together the various theories of al Qaeda financing, the group would have to be awash with millions of dollars from rough diamonds, gold, charitable donations, legitimate businesses and criminal enterprises including drug trafficking.

According to CIA estimates accepted by the 9/11 Commission as reasonable, al Qaeda had \$30 million per annum for the overall organization. For this size of funds - most of which need to be raised internationally and, thus, require fund transfers - the type of financial controls introduced in the aftermath of 9/11 are not unreasonable.

On the other hand, al Qaeda operatives have been found to be under-resourced or required to raise their own funds for operations. As al Qaeda departed the Sudan for Afghanistan, many operatives were left behind for the group could not afford their modest salaries. The militants behind the first World Trade Center attack regretted not having a few thousand dollars more to pack additional explosives and increase their impact. This is all at a time when very few governments or agencies were paying close attention to terrorist finance.

So, how much money is currently available to al Qaeda or other groups, when the international community is mobilized against terrorist finance? How much is available to other groups and threats? The lack of precise answers to these questions points to the need for a more systematic search for and evaluation of information on seizures, estimates of net worth, fund raising capacities, number and type of sympathizers, etc.

We have seen the importance of differentiating between the funding of particular operations and the funding for an organization or movement. Depending on the length of life, size and objectives of a group, large infrastructures may be necessary to support its activities. Many insurgent and militant organizations have had extensive recruitment, arming, training, command and control, welfare, education and social work, intelligence and other functions to perform, especially when they succeeded in bringing geographic areas under their direct control (IRA, LTTE, Hamas, Hizbollah, FARC, etc.). The target and context is very different, when it comes to individual operations, which are most often very inexpensive. In many instances, these can be self-financed and low budget.

We have also seen that between a tiny or marginal group and a large organization with substantial infrastructure, there are also networks of support, such as those fuelling the insurgency in Iraq as described earlier. Calculating the cost of suicide bombings in Iraq, would have to consider not only the explosives and intelligence gathering or other preparations for attacks, not only the travel expenses of a foreigner into Europe, Iraq or other places, but also the general/operating costs of a network procuring suicide bombers. In this particular case, we noted an observed interface with contraband and drug trafficking.

Most of the current CFT measures may affect the larger and resource-rich type of groups<sup>154</sup>, but do very little against the smaller ones (other than *ex post facto*). Current CFT measures cannot help much with finding amounts or value that can be carried in one's pocket and may not even have to be declared. In other words, we may have devised and implemented financial controls that are inadequate for some of the tasks at hand. When we are looking for a needle in a haystack, the use of a huge and wide pitchfork will not be particularly helpful. The truth is that small amounts cannot be stopped. To the extent that al Qaeda inspired actors are in the second group category, intelligence/monitoring/demand side measures are much more critical than financial controls.

So, we need to sort out who exactly is the target and what is their social organization, in order to fine tune our policy instruments accordingly. Yet, details regarding the amount of money involved in terrorist financing and how exactly resources are distributed within and between terrorist organizations remain limited or unreliable. As a result, it is difficult to determine which financial controls may be more useful (whether we should be targeting larger or smaller sum transactions, for instance) and where the focus of these controls should be directed (e.g., money services businesses, banks, or trade institutions). This imperfect knowledge affects resource allocation and priorities in counterterrorism and other areas of public policy.

A related point in this respect is also that the objectives and functions of financial controls must be well understood, and particularly the point

---

<sup>154</sup> In those instances, one would also have to consider the implications relative to non-combatant populations affected by such measures. For instance, what (de-)escalation effects would be generated by decisions on strict controls against groups controlling populated regions affected by natural disasters, poverty or other serious problems when the governments in charge are unable to unwilling to assist?



that intelligence gathering and investigative leads are the key goals, rather than 'drying up' the financial resources of terrorism, which is an impossible task.

## Identifying the Highest Risks and Trade Transparency

Because everything has been used to fund one terrorist activity or another, special interest groups fighting against particular problems seek to connect their issue with terrorism in order to gain support for their cause. Their commitment and good intentions notwithstanding, counter-terrorism policy and priorities ought to be set in as objective a manner as possible on the basis of good evidence and sound analysis. The same applies to governments seeking external support for the suppression of their political opponents at home, by alleging connections between local groups and al Qaeda.

It is potentially quite damaging to let priorities set themselves thanks to the differential persuasive or other power of particular groups acting against drug use, counterfeit products, a particular group that may not pose as strong a threat (or no threat) to North American interests, etc. For example, allying ourselves too readily with some Central Asian authoritarian government against groups, such as Hizb-ut-Tahrir<sup>155</sup>, can have the effect of radicalizing that group and creating a fertile ground for recruiting more militant and violent actors (e.g., for the IMU).

It is unclear, however, which terrorist groups rely mostly on which sources, under what conditions, in collaboration with what actors, and how/when do they adjust when particular controls and measures affect their operations. Also unclear is whether certain regions, type of goals or targets and ideological inclinations favor some methods or associations compared to others. An attempt was made earlier to offer a springboard through a typology of interfaces between criminal enterprises and terror groups. This, however, is but a starting point based on a preliminary review of a variety of sources the reliability of which cannot be guaranteed at this stage.

Necessary for the support of strategic and operational CFT initiatives is a program or a tool that evaluates the quality and strength of terrorism finance information so that actions against sources of terror finance may be better targeted, prioritized, coordinated, and effective. This may occur

---

<sup>155</sup> See Rashid, A. (2002). *Jihad: The Rise of Militant Islam in Central Asia*. New Haven: Yale University Press.

with respect to some intelligence material, but it has not been done with respect to open source data.

The lack of confirmed and validated information about terrorism finance limits the effectiveness of CFT efforts. Canadian authorities have stressed the integration of the various agencies involved in counter-terrorism. This may be the case in Canada, but not everywhere else. Limited intelligence distribution to different domestic agencies and overseas counterparts is a long standing problem that could be resolved through the use of a terrorism finance database supported by open source information. Another obstacle to effective CFT is the intelligence community's reluctance to integrate open source information into their analyses. While true that open source information is often misleading and biased (we have seen this), it can provide the context against which classified information can be interpreted, aid in the verification of classified information, and offer information where classified data are unavailable. Importantly, open source information also helps the intelligence community assess the knowledge base and inherent biases of presumed subject matter experts. Misinterpreted intelligence, whether from classified or open sources, can lead to strategic and tactical errors.

There is a lot of public information, which can be usefully collected and analyzed by or for intelligence and law enforcement agencies. The analytical task would have to involve *inter alia* a careful scrutiny of experts and their writings, so that not all sources are thrown in indiscriminately. A critical review process can identify possible conflict of interest, inconsistencies, lack of updates, mistakes and partial coverage of issues. In this way, users of such a database could access to both the raw material and a screening they could benefit from.

The determination of sources and associations of terror groups would also be assisted by an analysis and mapping of illicit networks. In addition to the tentative typology presented earlier, it must be noted that offenders rarely specialize in one kind of crime. Their involvement in a variety of illegal enterprises and offenses complicates the specialized law enforcement agencies that devote themselves to particular types of crime. Additional challenges are posed by:

- Difficulties in ascertaining the validity and reliability of information at the center of such cases. Often information is treated as 'fact' by virtue of simple repetition and not double-checked for accuracy even by scholars and policy analysts;

- Jurisdictional firewalls against the effective flow of relevant information and knowledge, which can slow down investigations;
- A narrow and limited focus on particular offenses may lead to a neglect of ways in which a variety of serious crimes may be committed by or through the same actors and networks<sup>156</sup>.
- The fact that there is no initiative to collect, organize and analyze in a systematic and comprehensive fashion data available through courts, media, scholarly outlets, think-tank, government or other reports.

What is thus called for is a project designed to do this work and to map terrorism and illicit networks. This sort of knowledge basis would inform multi-level and multi-lateral strategies and responses against terrorism and other serious crimes in ways minimizing collateral damage and maximizing synergies and efficiencies. This project will examine such processes as division of labor across and within illicit networks and will examine the ways in which illicit networks transcend geographic location, both within and across national boundaries. It would further facilitate analysis, studies of adjustments and shifts in terrorist finance methods, risk assessment, as well as anticipation<sup>157</sup>.

This initiative would also support an “Al Capone strategy” against terrorism; in other words, incapacitation policies could be facilitated by prosecutions on charges of terrorist finance or several other crimes against those deemed by intelligence to be the greatest threat. At the same time,

---

<sup>156</sup> The background to the London 2005 bombing illustrates this problem. MI5’s surveillance of a group of suspected terrorists led to the detection of another group. Both groups were photographed during four meetings across the London area. However, the ‘new’ group at the time was dismissed as less of a threat than the suspected terrorists (i.e. labeled merely ‘criminal’) because the discussions between the two groups related to ‘criminal’ matters, and not ‘terrorism’. In fact, that group that was categorized as ‘criminal’, and therefore thought to pose less threat than the suspected terrorist grouping, was eventually revealed to be the four-man cell that blew themselves up in July 2005, killing 52 people and wounding several hundred. What was in reality an extended illicit network, was downgraded in importance because of narrow assumptions about the nature of terrorism, the nature of involvement in terrorist activity and about the nature of criminality (Many thanks to my good colleague Prof. John Horton for drawing my attention to this illustration).

<sup>157</sup> A study of likely terrorist finance scenarios was conducted by German police authorities with support and participation from the European Union, Europol, private sector and academic experts; see EDGE 2007 Report on *Criminal Money Management as a Cutting Edge between Profit-Oriented Crime and Terrorism: Possible Developments until the Year 2012 and Strategic Recommendations*. Published by Landeskriminalamt Nordrhein Westfalen and the European Commission AGIS Programme.

well founded charges and prosecutions would prevent premature actions and unnecessarily aggressive measures against innocent parties or those who may be guilty of minor misconduct but having nothing to do with terrorism. To a certain degree, the reliance on a broad, deep and high quality information base would turn crime control into very effective and fair counter-terrorism.

The question of how to merge law enforcement and intelligence work is a hard one to resolve, especially when it comes to security matters. Different methods, approaches, functions and mandates do not make it easier. An evidence-based and analysis-guided approach, however, enables appropriate interactions between intelligence and law enforcement. Intelligence combined with open source information can better guide law enforcement actions, which can further develop the sort of evidence that can be shared more widely and presented in courts.

Another advantage of broader informational support is that more precise and useful guidelines can be offered to controllers and private sector about priority areas and indicators of abuse or suspicious activities that must be reported to authorities. For example, charities and informal remittances are sectors we discussed briefly earlier.

## **Charities**

With regard to charities, the UK Charity Commission has offered the following indicators of suspicious activity, which should be taken into consideration in other jurisdictions as well:

- “If offered large donations from persons unknown to the trustees, the trustees may wish to make further enquiries before accepting the donation, and may refuse a donation if satisfactory replies to enquiries are not received
- Donations conditional upon particular individuals or organisations being used to do work for the charity may be refused
- Offers of donations in cash, for a certain period of time, the charity to receive the interest, but the principal to be returned to the donor at the end of the specified period, may be refused



- Donations in foreign currencies, with the provision as above, but the principal to be returned to the donor in the form of a sterling cheque, should be refused”<sup>158</sup>

As the 9/11 Commission report pointed out, a fundamental issue raised by the US government’s approach to combating terror financing is “the problem of defining the threshold of information necessary to take disruptive action.” We certainly need to distinguish “the difference between seeing ‘links’ to terrorists and providing the funding for terrorists.”

An approach that merits some consideration is the following. Once intelligence interpretations suggest that a charitable organization supports a terrorist group, one could systematically monitor its activities in order to identify the donors and establish their knowledge, the intent of principal charity actors, the channels and jurisdictions through which funds go and activities take place, the final destination and social organization of receiving groups, etc. In this way, if the intelligence interpretation is correct, authorities will be able to prevent attacks, collect valuable information on the *modus operandi* of a terror group and its sources of support, gather the evidence which can be used in a court of law, and bring criminal action as soon as deemed useful and necessary. If the intelligence interpretation proves to be incorrect, then no unnecessary collateral damage would be caused.

## Hawala and Informal Sectors

With respect to hawala and informal economic issues in general, it is important for countries to assess as accurately as possible the extent, nature and activities in their informal economic sectors. Careful analysis can furnish insights and knowledge that may be counter-intuitive. For instance, research based on both public and non-public data has shown that, while *transparency* of hawala-like networks is comparatively low, *traceability* of transactions by competent and well-informed/trained investigators is often very high<sup>159</sup>. Traceability may be achieved by means other than formalization, computerization or centralization of data. In other words, knowing where to look and what questions to ask

<sup>158</sup> Operational Guidance; Charities And Terrorism, Og 96 – 29 August 2007, <http://www.Charitycommission.Gov.Uk/Supportingcharities/Ogs/G096.Asp>

<sup>159</sup> We have seen earlier why it is important to distinguish between transparency and traceability of transactions.

is of critical importance<sup>160</sup>. Details on customers, beneficiaries, dates and amounts may be accessible to controllers, even if the informal financial service providers are not regulated in the same way as formal institutions. In other words, it is better to pursue maximum traceability than over-concentrate on transparency and thereby marginalize operators who may cooperate.

Criminal abuses of hawala may be investigated more easily than generally assumed. Because they interface with formal banking institutions, fund transfers can be tracked. The frequent fax and telephone traffic among hawala agents and their clients, intermediaries and counterparts creates monitoring opportunities and trails that can be followed. More importantly, hawala agents leave paper trails at home or in business premises. Often, they keep detailed ledgers with transactions for legitimate clients, while suspicious transactions may be recorded in shorthand or codes.

Secondly, informal fund transfer methods are attracting just as much attention from intelligence and law enforcement agencies as do formal channels. Seasoned investigators in South and Southeast Asia and the Middle East have always been aware of the significance of such networks for terrorist finance and other misconduct. In the West, the regulatory response has shifted from earlier neglect to exaggeration and miscalculations of comparative risks, costs and AML/CFT benefits of recent measures, some of which may have undercut counterterrorism efforts<sup>161</sup>.

Thirdly, the operation of some international and global terror groups notwithstanding, many terrorist groups and their operations are local, thereby necessitating no funds *transfers*. To the extent that fund raising and expenses are in the same place, what would be the purpose of any transfers? In addition, if an inexpensive terrorist attack is planned and executed, even if the perpetrators have some international associations or connections, the funds may be raised locally, again without the need for any transfer. One of the suicide bombers in London left behind savings and investments that could have been used for their attacks, but this apparently was not necessary. This points up yet again the importance of a) establishing the social organization and methods of terrorists groups

---

<sup>160</sup> See Passas, N. (2006). Demystifying Hawala: A Look into its Social Organisation and Mechanics. *Journal of Scandinavian Studies in Criminology and Crime Prevention* 7(suppl. 1): 46-62(7(suppl. 1)), 46-62; see also Passas, N. (2008). Dirty Money: Tracing the Misuse of Hawala Networks. *Jane's Intelligence Review* (13 February), <http://jir.janes.com/public/jir/index.shtml>.

<sup>161</sup> Passas, N. (2006). Fighting Terror with Error: The Counter-productive Regulation of Informal Value Transfers. *Crime, Law and Social Change*, 45(4-5), 315-336.

and particularly the nature and extent of international/global linkages, *if any*; and b) assessing and prioritizing a government's terrorist threats, so that resources can be allocated to the most immediate and important problems.

Fourthly, it is essential to note that hawala is not necessarily the preferred mechanism for terrorist funding transfers. The formal banking and funds transfer system (such as Western Union, Moneygram, etc.) has often been exploited as well.

In conclusion, hawala is a vital vehicle for expatriate remittances to their homeland, an important instrument facilitating trade and a development tool, as well as a means for terrorist financing and other misconduct. Contrary to conventional wisdom, hawala offers unique opportunities for monitoring illicit networks, investigative leads and traceability<sup>162</sup>. Some of the proposed policy responses to these challenges include:

- Encouraging banks and other formal institutions to stop being overcautious when dealing with Money Service Businesses (MSBs) and ethnic remitters. This can have the effect of forcing such businesses to go underground.
- Diversifying rules applicable to different service providers.
- Simplifying and harmonizing rules and regulations at the national and international levels.
- Paying more attention to traceability means that formalism should give way to pragmatism; effectiveness ought to be a higher priority than paper compliance and window-dressing. Unnecessary rigidity of rules applicable in diverse contexts must be avoided; initiatives seeking region-specific AML/CTF approaches consistent with United Nations, Financial Action Task Force (FATF) or other international standards as well as economic or other policy objectives need to be encouraged.

---

<sup>162</sup> For example, investigations such as those of the attacks on the Indian Parliament and of the recent bombings in Mumbai made progress because hawala transfers for the operational costs furnished information on the conspirators.

- In federal states, it is imperative that different jurisdictions and agencies coordinate and synchronize their efforts in consultation with the concerned sectors.
- The economic and social role of remittance providers needs to be publicized. Banks could be offered incentives, so that they maintain old and open new accounts for legitimate and compliant MSBs.
- Define the role of banks with respect to due diligence and risk management, avoiding the impression that they are expected in practice to police MSBs.
- Offer incentives for high quality and well implemented AML/CFT programs at banks and MSBs.
- Enforce rules consistently and with due process by keeping line agents and bank examiners aware of amended rules, updated guidelines and best practices.
- Law enforcement actions must be taken on the basis of evidence that may be produced in a court of law. As in the case of charities, when evidence is not 'actionable' or originates from non-shareable intelligence, one could follow the money and monitor activities.

Studies based on combined open source and non-public information have produced a list of red flags relative to informal remittances, which can be used by regulators, controllers as well as the private sector:

- Different commission charged to ordinary clients
- Different recording methods for some clients
- No recording of certain (large) transactions
- Large sums (from single customer)
- Different collection methods



- Transactions divergent from usual pattern (such as very large amounts once in a while)
- Transfers to companies in a very different business
- Transfers to accounts of individuals or companies involved in illegal activities<sup>163</sup>.

## Trade Transparency

Other work based on combined public and non-public information offers additional insights needed for risk assessments. We noted earlier how some publications drew attention to the role of diamonds and other natural resources in terrorism finance, while unfortunately being misleading on the extent, type and location of the highest threats. At the same time, research into precious stones, precious metals and tobacco revealed serious vulnerabilities in the commercial sector in general due to lack of transparency and many uninvestigated irregular trading practices. Consistently with calls by the FATF and other policy bodies for consideration of trade-based financial crime<sup>164</sup>, this work suggests that the highest priority regarding financing militant threats stems from certain trade-facilitated types of informal value transfer systems (IVTS)<sup>165</sup>.

Interviews with Customs officials and analysis of US import data demonstrate that there are serious gaps in the way the US and all other governments deal with trade transactions. Incomplete, erroneous or illegal documentation can be found through routine review of forms filed with Customs authorities. Inattention, lack of adequate resources and expertise, high transnational volumes and complex rules and regulations add to the challenge.

<sup>163</sup> Passas, N. (2004). Indicators of Hawala Operations and Criminal Abuse. *Journal of Money Laundering Control*, 8(2), 168-172.

<sup>164</sup> See FATF 2006 "Trade Based Money Laundering Report" available at <http://www.fatf-gafi.org/dataoecd/60/25/37038272.pdf>

<sup>165</sup> Passas, N. (2003). *Informal Value Transfer Systems, Money Laundering and Terrorism*. Washington D.C.: Report to the National Institute of Justice (NIJ) and Financial Crimes Enforcement Network (FINCEN); Passas, N. (2004). *The Trade in Diamonds: Vulnerabilities for Financial Crime and Terrorist Finance*. Vienna, VA: FinCEN, US Treasury Department; Passas, N. (2006). Setting Global CFT Standards: A Critique and Suggestions. *Journal of Money Laundering Control*, 9(3), 281-292; Passas, N. (2006). *Terrorist Finance and the Nexus with Transnational Organized Crime: Commodities Trade*. Washington D.C.: Report to the National Institute of Justice (NIJ); Passas, N., & Jones, K. (2007). The regulation of Non-Vessel-Operating Common Carriers (NVOCC) and Customs Brokers: Loopholes Big Enough to Fit Container Ships. *Journal of Financial Crime*, 14(1), 84-93; available at <http://www.emeraldinsight.com/Insight/viewContentItem.do?contentType=Article&contentId=1585488>

The skills, experience and opportunity to raise funds and transfer them across borders through trade undetected are available in many corners of this planet with sympathizers for groups aspiring to acquire capacity to inflict serious harm on national and international community interests. It only takes a handful of sympathizers to exploit the current gaps in trade transparency and the resulting lack of accountability. Mis-invoicing alone can serve to transfer significant funds without detection. Unfortunately, nominee trade and obscure value transfers can occur in billions of dollars in ways not detected or fully understood by the authorities.

If a serious security concern for the future is the possible use of WMD by terrorists or other proliferation issues, the 'black box' that trade represents must be addressed as a matter of extreme urgency. So, it is strongly recommended that we devise and implement measures aimed at enhancing transparency, traceability and accountability in all trade. It is essential to note that concentrating too much and prematurely on particular economic sectors would risk unnecessary costs on the affected industries and would enable the undetected commission of serious misconduct through other routes, while creating the illusion that trade vulnerabilities to terrorist finance have been addressed.

The technology for beginning to monitor trade and to red-flag irregular transactions already exists and has been used by US and other Customs agencies in the past, but not consistently or systematically and with the necessary support<sup>166</sup>. Import and export data can be compared to see whether they match (they almost never do), offering the opportunity to examine the reasons for such asymmetries and strategically or tactically use the information. Analyses of such discrepancies and their displacement following law enforcement actions can provide invaluable support for proactive and reactive investigations as well as for monitoring activities and anticipating moves. Trade raw data of course are far from perfect and entirely accurate themselves. This method, thus, is not a panacea, but a solid and promising beginning.

At the present time, there are trade data in addition to the official records and material used by governments with the software program. The program integrates and compares import and export data with other material, such as suspicious activities reports, reports on cash transactions, reports on cross-border cash movement, reports of criminal

---

<sup>166</sup> The software program NIPS (Numerical Integrated Profiling System), now renamed Leadminer is available to the US Trade Transparency Unit at the Department of Homeland Security as well as some overseas counterparts.

investigations, information on ongoing investigations, criminal records, etc.<sup>167</sup>. However, shippers, brokers, exporters and importers keep their own records anyway. These records would complement and confirm official sources. More importantly, they would also add insights into where identified irregularities are located and where explanations can be found. That is, if exported containers do not appear in import records of the relevant country, the diversion may have occurred at different transshipment points, which can be established only through these other records.

Two major benefits would be gained by such trade transparency initiatives. Firstly, there will be no need for all countries to participate and contribute to such knowledge or information exchange. If several neighboring countries share their trade data, then the dots can be connected more easily even with regard to jurisdictions where governance and Customs capacity need improvement. Effectively, this initiative would shed light on commercial flows that remain currently obscure.

Secondly, once commercial flows become more transparent and traceable, they could be compared and matched with financial and messaging flows, which are more closely monitored now, but independently. Consequently, the effectiveness of AML/CFT will improve drastically.

Finally, as with the financial sector, control objectives can only be achieved with the active and willing cooperation of the private sector and traders who are often in the best position to spot irregularities and notify authorities. This cooperation can be enhanced and maximized when private actors perceive the control system as appropriate and necessary, which brings us to the question of consensus building and legitimacy.

## **Legitimacy of CFT**

The success of any policy depends on the degree to which participants and stakeholders believe that it is necessary, appropriate and effective. For some, legitimacy is a matter of moral and legal principle on its own, a goal in itself. For others, it is an instrument towards the achievement of wide and genuine international collaboration. Either way it is a necessary condition for effective policies and long-term success. CFT measures must enjoy legitimacy, which can be strengthened through partnerships

---

<sup>167</sup> See Appendix for more information on the software program.

with the private sector and civil society, outreach, integration and coordination of government efforts, accountability, alignment with other public policies and fundamental legal principles at the domestic and international levels.

## Partnerships and Outreach

Government partnerships with the private sector and wider society are indispensable for the goals of prevention, transparency and traceability to be achieved domestically and internationally<sup>168</sup>. In a sense, the best counter-terrorism we can think of would come as close as possible to a community policing approach, where everyone works together and makes distinct contributions in comparative harmony.

The best way of earning private cooperation and collaboration is by formulating responses through outreach and consensus building (to the extent possible) and then implementing them without overburdening either the private actors or government agencies with rules and procedures that cost a great deal and produce little result.

For example, with respect to informal and ethnic remittance services, government agencies' statements and actions are occasionally inconsistent. While the economic and social role of money service businesses is recognized, outreach efforts have been limited and rather one-way communications of new and poorly explained duties and responsibilities. Whenever all stakeholders are invited to participate in a consensus-building process, the expected compliance rate and effectiveness of measures can be much higher. It is possible that charities and financial institutions of different sizes, operating in different parts of the world, dealing with different legal or geo-political conditions, performing different functions, etc. will be able to suggest processes and practices in differentiated and proportionate ways with which they can live and which also serve the security and crime control needs. They may even become more proactive and report on suspicious activities not previously considered by the authorities.

On the other hand, over-zealousness and strict enforcement for unachievable and non-pragmatic objectives may backfire: fewer people

---

<sup>168</sup> It is still undecided on how government agencies ought to interface with financial institutions regarding classified information. Giving clearance to bankers is an idea rejected by the 9/11 Commission, while gaining access for counter-terrorist finance purposes only on ad hoc basis cannot be accomplished on the basis of current technologies and infrastructure.



may see the need for particular controls, shun heavy paperwork and reporting requirements, resent unclear guidelines on “suspicious transactions”. They may not see such measures as necessary and therefore regard them as less legitimate or binding. Overburdening private actors and government agencies with rules that produce little result undermines legitimacy, while measures may miss their target. For example, bank compliance officers and government officials have confirmed in interviews the 9/11 Commission’s finding: the 9/11 hijackers’ financial activities were not unusual, did not trigger reports by financial institutions and should not have done so either. Even if current rules were in place before 9/11, including the FATF nine special recommendations, the terrorist transactions would not have been red-flagged. This begs the question of what adjustments must be made.

Further, we need to transcend the notion that one set of standards can be equally productive, useful or applicable throughout the world. We must always consider the context of each region, prioritize sectors to be regulated by risk, and avoid formal and legalistic criteria of compliance rather than judging the effect and efficiency of measures on the substance.

Moreover, we need to recognize that countering terrorist finance is not the same as anti-money laundering. Money laundering is when dirty funds are intended for legitimate use and need to show a legally acceptable origin. If funds, dirty or clean, are to be used for criminal purposes, there is no need for laundering them. Gun runners and nuclear proliferators do not ask for receipts or explanations on the provenance of funds. Secondly, the amounts we are attempting to control pale by comparison to the volume of criminal proceeds laundered, therefore mechanisms and expectations must be differentiated. Thirdly, many argue that we have had only moderate successes even with respect to AML efforts. Therefore, adjustments need to be made for both CTF and AML. Fourthly, the process of terrorist finance is often the reverse of money laundering, when clean funds are used for evil acts. It is after the fact and for monitoring purposes that we need certain controls in place, because otherwise there is little irregular or uncommon about the transactions before the identification of terrorist actors. Finally, to the extent that we go on designating supporters of terrorist groups and freezing or seizing of their assets, sympathizers willing to offer financial support will wish to cover their name and the origin of their funds. In such scenarios, it is plausible to assume that infrastructures and methods employed by

money launderers may also be used for terrorist finance. Hence the need to constantly update our understanding of these methods, to try to anticipate their next moves and to keep an eye on the participants in this illegal market.

## **Integration and Coordination of Efforts**

Short-term responses must be combined with long term policies and measures in order to address some of the root causes of terrorism. CFT is a supply side approach to counter-terrorism which must be accompanied by a demand side approach too. Understanding the reasons why militants emerge, persevere, resonate with larger social groups, evolve and radicalize or de-escalate their activities are all essential. In this spirit, we also need to understand and appreciate the consequences of financial controls domestically and internationally.

Proper regulatory measures are best developed when we avoid ethnocentric thinking. For instance, many efforts were made to see whether reports about short covering of airline and other stocks before 9/11 was practiced by militants as a fund-raising method. We absolutely must think of all possibilities and cover all bases. However, our thinking must not be constrained by our own context and experiences. As the 9/11 Commission reported, there was no terrorist involvement in short covering after all. We need to think “outside the box” and put ourselves in the shoes of the militants in as realistic a fashion as possible.

In this process, it is vital that we avoid or minimize “collateral damage”. As noted below, unrealistic and aggressive practices against ethnic money remitters may a) not produce any results or help make the homeland more secure and b) alienate communities that would otherwise be inclined to join in coalitions against terrorism. At the very least, we would not be creating new motives for sympathizers and outsiders to support or turn a blind eye to terrorist actions.

Every country is faced with multiple regulatory requirements due to a number of international instruments which have come recently into force, including not only UN the convention and Security Council Resolutions regarding terrorist finance, but also the UN convention against corruption, the UN convention against transnational organized crime, the FATF Recommendations and many others. As a result, both governments and private actors have been overwhelmed by what I have

termed a “regulatory tsunami”. In this context, it is imperative to find synergies among those instruments by coordinating the implementation of mandatory and other requirements. It is also important to keep in mind and enforce CFT consistently with other broad social policy priorities, (such as economic growth and development, poverty, environment, public health, conflict).

Finally, networked terrorist actors demand a networked response. Counter-terrorism these days necessitates multi-agency and international efforts. This is easier said than done, but the mutual benefits for security and crime control will hopefully prove conducive to more effective international cooperation.

### **Accountability**

We have seen how the effectiveness of AML measures was questioned by government officials before 9/11 and yet the same or similar measures have been used without question against terrorist financial. The logic of cost-benefit considerations underlying the earlier critical spirit would be usefully applied to current CFT approaches, in order to determine at what point we face an issue of diminishing returns.

In view of the previous recommendations relative to evidence-based policy-making, one could also envisage regular assessments and adjustments as needed. As terrorist methods change, so must the response. In this process, we could introduce reasonable qualitative and quantitative yardsticks of progress, which could be used also as self-assessment tools by government agencies.

### **Compliance with Fundamental Legal Principles**

Finally, premature and aggressive actions can create a climate of pressure to prevent disclosure of exculpatory evidence or admission of mistakes in the process. It is in such climate, for example, that former chief military prosecutor at Guantanamo Bay, Air Force Col, Morris Davis was so upset

with the process and conditions that he turned into a defense witness for bin Laden's driver<sup>169</sup>.

The point is that we can not win the battle against terrorism if we undermine our own fundamental legal principles. We cannot defend democracy, human rights and due process by undermining them domestically or internationally. All countries must make sure that errors made by themselves or other countries be detected and corrected. Canada has set great precedents by properly refusing to satisfy international legal assistance requests in the Barakaat case, which lacked foundations, and by taking appropriate remedial actions in the Arar case.

Legitimacy will be generally strengthened and preserved as we make clear and visible efforts to act on the basis of solid evidence and sound analysis, minimize negative consequences of CFT policies for innocent actors, protect constitutional rules, and observe our legal rules and international standards.

## Conclusion

In short, CFT is necessary and vital, but we must have realistic expectations and targets. We may have been successful in some respects, including the neutralization of al Qaeda's infrastructure in Afghanistan, but many aspects of CFT need re-thinking and re-adjustment. This need is based not only on the basis of legal, ethical or moral grounds but also because of the net results for economic, political, physical and other interests of Canada and the international community. In some respects, we have been fighting terror with error causing collateral damage to ourselves.

It is essential to bear in mind that, in many ways, terrorism is cheap and that small amounts will never dry out for any militant cause. We have to clearly identify our main problems and targets, collect and analyze

---

<sup>169</sup> Col. Davis has been reported as affirming that "Pentagon general counsel William Haynes said in August 2005 that any acquittals of terrorism suspects at Guantanamo would make the United States look bad, calling into question the fairness of the proceedings. ... "He said 'We can't have acquittals, we've got to have convictions (see Fox, B. (2008). Ex-Guantanamo Prosecutor to Aid Detainee. *ABC News* (February 21), <http://abcnews.go.com/TheLaw/wireStory?id=4326458>). See also how politics has contaminated the military commissions in Mark Falkoff (2008) "Politics at Guantanamo: The Former Chief Prosecutor Speaks" available at <http://jurist.law.pitt.edu/forumy/2007/11/politics-at-guantanamo-former-chief.php>; see also former administration official's accounts making similar points: Clarke, R. A. (2004). *Against All Enemies: Inside America's War on Terror*. New York: Free Press; Goldsmith, J. L. (2007). *The Terror Presidency: Law and Judgment inside the Bush Administration*. New York: W.W. Norton & Co.



critically the evidence on their *modus operandi*, motives, aims, financing and support, and then to focus on carefully planned and consistently applied policies that are instrumental to our goals and minimize the externalities and adverse effects.

We must keep working to facilitate monitoring and to enable investigations as well as to enhance cooperation within and across national borders. We must not lose sight of our critical intermediate goals: to maximize compliance, to increase transparency and traceability in economic transactions (both financial and trade) and to control crime of all sorts. An important as yet unaddressed vulnerability is that of trade transparency; dealing with that problem is imperative and urgent. These goals can be attained through reasonable, pragmatic, realistic policies, which are based on consensus building efforts with the private sector, do not alienate communities and allies, and enjoy wide legitimacy.

In most areas of public policy, there are very difficult zero sum calculations to consider. The optimistic conclusion of this report is that with respect to CFT we either have win-win or lose-lose options. This should not be a hard decision to make.

## Appendix: Two Solutions

The trade non-transparency issues discussed in the report have clear implications for a global CFT strategy. Low and locally raised amounts entail no or lesser need for cross-border fund transfers. Cross-border communications may be fewer and the use of intelligence on one particular group may be less relevant to other groups. Ordinary crime (petty and large scale) is very likely to be used for fund raising.

All this points to the increased importance and potential role of sympathizers as well as the significance of ideological, political and socio-economic factors. Implementing ways in which 'community policing' approaches to counter-terrorism can be enhanced and strengthening alliances supportive of efforts to prevent terrorism are crucial.

This renders clear how crucial a role the larger society and especially the private sector can and should play. Stakeholders and active participants in the financial and commercial business are aware of irregular and suspicious patterns and transactions that may be extremely helpful to controllers. They should also be made more familiar with additional patterns and trends identified by the authorities.

The small amounts which we have seen are quite sufficient to cause serious harm and societal damage will never dry out for extremist and militant causes. We have discussed the need to clearly establish each country's main problems and targets, collect and analyze critically the evidence on the militants' modus operandi, motives, aims, financing and support, and then to focus on carefully planned, consistently enforced and fairly applied policies that are instrumental to our goals and minimize the negative externalities.

We must keep working to facilitate monitoring and to enable investigations as well as to enhance cooperation within and across national borders. We must not lose sight of our critical intermediate goals: to maximize compliance, to increase transparency and traceability in economic transactions (both financial and commercial) and to control all types of crime.

In this context, trade transparency ought to be given a very high priority. Addressing adequately and squarely this problem is imperative and urgent. The CFT goals outlined in the main report can be attained through

reasonable, pragmatic, realistic policies, which are based on consensus building efforts with the private sector, do not alienate communities and allies, and enjoy wide legitimacy.

As all countries are under pressure to introduce and apply international standards on multiple issues and deal with a 'regulatory tsunami', it is necessary to seek and take full advantage of all synergies with respect to the implementation of overlapping provisions and functions. Governments, pursue other goals too: security, peace, good governance, human rights, poverty, economic growth and development, public health, environmental protection, etc. As we move towards global CFT standards we must recognize the externalities of some current policies and avoid "regulatory fundamentalism", that is the persistent and thoughtless application of ineffective and/or counter-productive measures.

At the present time and in many countries, the right balance has not yet been found. Discontent and anxiety about the current regulatory arrangements can be found in all circles (e.g., among banks, money service providers, migrant communities, traders, regulators, law enforcement agencies, non-profit organizations, the public and the international community). As argued in the main report and elsewhere, we must scrutinize presumed "experts", engage in evidence-based threat assessment, offer better guidance to the private and non-profit sectors, and apply existing human and technological capital to productive use. The lack of trade transparency has been isolated as one of the most significant vulnerabilities partly because it constitutes a serious threat on its own and partly because it simultaneously undermines all other regulatory efforts which are made relative to financial transparency and traceability as well.

This is where two available and inexpensive programmes/technologies can assist effectively and without any substantial additional paperwork or change in procedures, rules, or modus operandi. The private sector and scholarly contributions can assist in the effort to connect trade with finance. One may start with an analysis of known terrorist financial activities, establish red flags, and thereby enhance the utility of Suspicious Transaction/Activity Reports. In this way, such reports will not overwhelm financial institutions or inundate authorities with irrelevant or unused information.

The two promising private-sector initiatives on trade and on cross-border remittances are Leadminer and Distributed Capital. The former addresses

trade, the latter finance; they can both be used in parallel to allow almost complete transparency and traceability in both with the capacity to cross-check them and thereby generate economies of scale and immediate results.

### **“Leadminer”**

The skills, experience and opportunity to raise and transfer funds across borders undetected through trade are available in many places where sympathizers of militant or extremist causes live and operate.

The technology for better monitoring of trade and red-flagging of irregular transactions is in place and has been used by the US and other Customs agencies in the past, but not systematically or with the necessary support. The software program Numerical Integrated Profiling System (NIPS), which has been renamed Leadminer and has undergone constant development for additional functionalities, allows the parallel use of any database one wishes (or is cleared) to connect, such as import-export official data, PIERS and carrier records, suspicious transaction reports, criminal records, active investigations, cash transactions or transfers etc. Cargo and container movements, import and export data from different sources and countries can be compared and contrasted. This offers an opportunity to track transactions and operators, examine the reasons for discrepancies and use the information and analysis by commodity, region or subjects strategically and tactically. Analyses of import-export irregularities (e.g., in country of origin, destination, pricing or routing) and their displacement following law enforcement actions can support proactive and reactive investigations, the monitoring of suspicious and illicit activities and the anticipation of future moves by offending actors.

### **“Distributed Capital” (DC)**

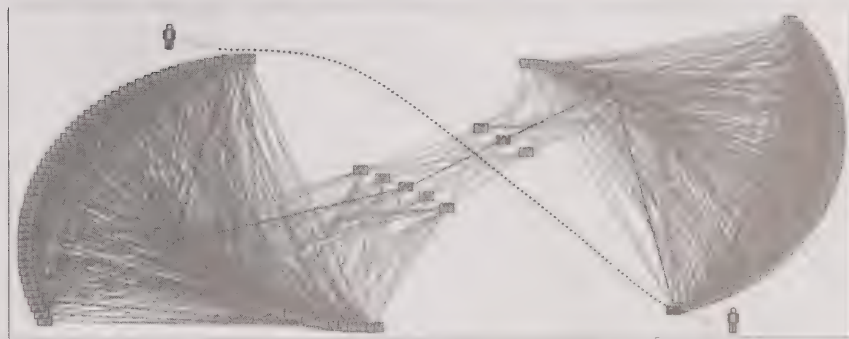
Informal networks are efficient, convenient, inexpensive, accessible, omnipresent and fast. Their business model relies on trust and integrates multiple trade and financial nodes in a global network. In part they also gain a competitive advantage when they also allow illicit transactions to go through (illegal actors or those who wish to hide something are prepared to pay a premium), which informal operators may take advantage of and thus be in a position to offer better rates to perfectly legitimate clients whose funds provide liquidity for the whole system. Transparency is not a distinguishing feature of informal networks, although they can be



quite useful with respect to tracing counterparties and transactions. This tracing, however, is labor intensive and requires skills and patience not always readily available.

Formal payment systems, on the other hand, are slower, more expensive and occasionally bureaucratic or inaccessible, at least in many parts of the world. Yet, they offer transparency and a degree of speedy traceability.

Distributed Capital seeks to combine the best aspects of the two formal and informal worlds. In essence, it attempts to provide a method drawing on the informal (hawala) business model with complete transparency. It also connects big with small financial operators and increases public access to financial services.

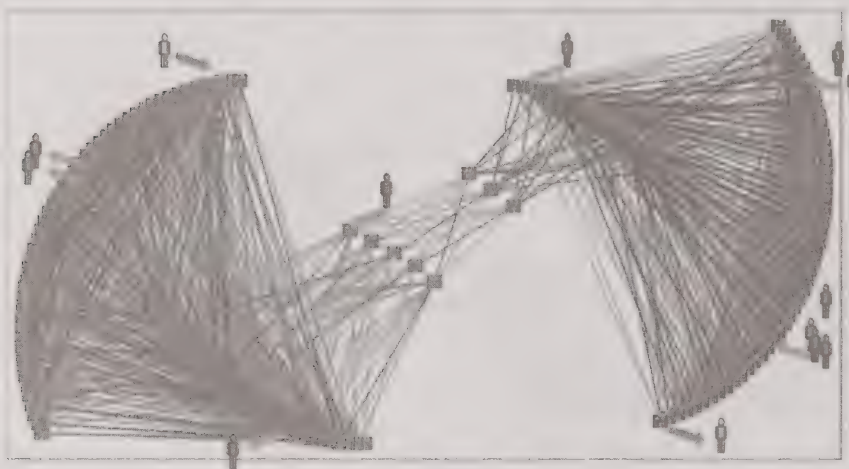


Graphic 1

Graphic 1 shows how a retail remitter sends money to someone in a different country. The dotted line shows the intended trajectory of the transaction, while the money gets to the final destination through a number of intermediary relays (red line). The green lines represent institutional connections or correspondent relationships, while the red line shows the actual travel-pathway of a payment over those relationships. This is how Money-Service Businesses (which use bank accounts) and formal banks route the payments.

Wherever there is more than one intermediary between the sending and receiving institutions, neither the sending nor the receiving institution has full transparency on which institutions the payment actually traveled

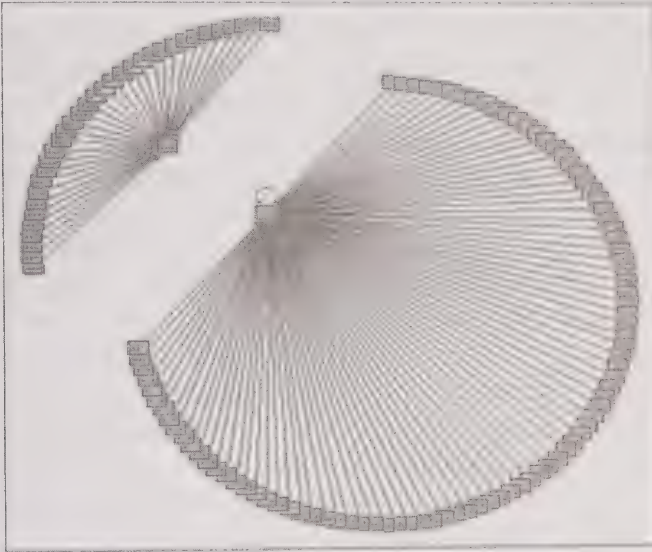
through. Given the number of permutations in a global network of thousands of participating institutions with multiple relationships, it is hard to track down all activity that occurs along these routes. Tracking crime that leverages this global complexity to engage in or facilitate terrorist finance or other illegal activity is difficult, expensive and time consuming. It also necessitates multi-jurisdictional efforts in order to reconstruct the complete transaction route. This drawback to conventional routing undercuts transparency. This is one feature or problem that Distributed Capital can help remove or reduce substantially to more manageable proportions.



Graphic 2

Graphic 2 depicts transfers in both directions. The blue arrows highlight the original intended payment, while the brown arrows illustrate payments made by other counterparties at about the same time. In the conventional bank network, each payment would be routed as illustrated by the red lines. If informal methods are used to execute these payments, however, we would see only or mostly local (redirected) payment flows. For example the outbound blue-arrow flow at top left can be re-routed locally to fulfill the inbound brown-arrow flow also at left (in the same country and currency).

Distributed Capital can implement effectively such local redirecting of capital flows in all jurisdictions simultaneously to deliver a more efficient payments processing. At the same time, it can record and monitor every intended payment alongside of the actual resolved set of instructions that deliver the local-rerouting method of settlement. The more institutions and jurisdictions/currencies use this platform, the more efficient the system becomes by minimizing further the need for cross-currency and cross-border transactions and eliminating the opaque settlement process that raises crime risks and concerns among controllers (see Graphic 3).



Graphic 3

These two solutions separately or combined will by no means solve all problems of traceability or terrorist finance. They do highlight however the progress and gains we can achieve through the use of existing technologies and through partnerships between the public and public sectors.

Nikos Passas is Professor of Criminal Justice at Northeastern University. His law degree is from the Univ. of Athens (LL.B.), his Master's from the University of Paris-Paris II (D.E.A.) and his Ph.D. from the University of Edinburgh Faculty of Law. He is a member of the Athens Bar (Greece). He is fluent in 6 languages and plays classical guitar.

He specializes in the study of financial/trade flows, white-collar crime, corruption, terrorism, financial regulation, organized crime and international crimes. He has published more than 100 articles, book chapters, reports and books in 11 languages. He is the author of Informal Value Transfer Systems (IVTS) and Criminal Activities (2004), Legislative Guide for the Implementation of the UN Convention against Corruption, Legislative Guide for the Implementation of the UN Convention Against Transnational Organized Crime (2003), IVTS and Criminal Organizations: Underground Banking Networks (1999) and the editor of The United Nations Convention against Corruption as a Way of Life (2007), International Crimes (2003), It's Legal but It Ain't Right: Harmful Social Consequences of Legal Industries 2004); Upperworld and Underworld in Cross-Border Crime (2002); Transnational Crime (1999), The Future of Anomie Theory (1997), and Organized Crime (1995). In addition, he has recently edited a volume on the Regulation of Informal remittance Systems for the IMF, co-authored a World Bank study into Migrant Labor Remittances in the South Asia Region, authored two reports to FinCEN on the trade in precious stones and metals and completed studies on procurement fraud, corruption asset recovery, as well as on governance, development and corruption international policy.

He serves as editor-in-chief of the international journal Crime, Law and Social Change and associate editor of the International Journal of Comparative and Applied Criminal Justice, the Open Criminology Journal, and the European Journal on Criminal Policy and Research. He is on the Board of Directors of the International Society of Criminology.

Passas offers training to law enforcement, intelligence and private sector officials on regulatory and financial crime subjects. He regularly serves as expert witness in court cases or public hearings and consults with law firms, financial institutions, private security and consulting companies and various organizations, including the Financial Crimes Enforcement Network (FinCEN), the IMF, the World Bank, other multilateral and bilateral institutions, the United Nations, the Commission of the European Union, the US National Academy of Sciences, research institutions and government agencies in all continents.



He is currently working on the regulation of free trade zones and of extracting industries, trade based financial crimes, money laundering and terrorist finance, the implementation of the UN conventions against transnational crime and against corruption, identity fraud and human trafficking. For example, he is the *Rapporteur General* on terrorism finance for the International Association of Penal Law Congress in 2009 in Istanbul, advisor of the Caribbean Financial Action Task Force, the UN Monitoring Group on Taliban and Al Qaeda sanctions, the Commission of the European Union, the UN Office of Drugs and Crime, the UN Development Programme, the Interpol Anti-Corruption Academy etc. His current projects focus on the development of a self-assessment tool for the implementation of the UN Convention against Corruption and the UN Convention Against Transnational Organized Crime and on research and analytical support for the International Association of Anti-Corruption Authorities (IAACA) and the creation of an international knowledge management consortium on corruption laws, cases, strategies, asset recovery and anti-corruption bodies.



## **AN ASSESSMENT OF THE LEGAL REGIME GOVERNING THE FINANCING OF TERRORIST ACTIVITIES IN CANADA**

**By**

**Anita Indira Anand\***

---

\* Anita Indira Anand, B.A., B.A., LL.B., LL.M., Associate Professor, Faculty of Law, University of Toronto. Opinions expressed are those of the author, and do not necessarily represent those of the Commission or the Commissioner. Thanks to Kent Roach for helpful comments and to Karen Andreychuk and Amy Murakami for valuable research assistance. Thanks to Patricia Marson for her assistance in preparing the document.





**TABLE OF CONTENTS**

1. Introduction	121
2. Canadian Regime	122
A. Criminal Code	123
B. Proceeds of Crime Act	127
3. United States	132
U.S. Criminal Code	132
Patriot Act	133
Money Laundering Statutes	135
The Bank Secrecy Act	136
Office of Terrorism and Financial Intelligence	137
4. Analysis	138
A. Problems with Current Regime	138
B. Directions	145
5. Conclusion	151



## 1. INTRODUCTION

This study analyzes Canada's legal approach to combating the financing of terrorist activities. It also undertakes a comparative discussion with U.S. law to isolate cross-country differences in legislative and procedural mechanisms designed to prevent terrorist financing. Underlying the legal discussion is an analysis of the role of, and costs imposed upon, the private sector in monitoring and reporting financial transactions; the balance between privacy rights and deterring the financing of terrorism; and, the need to assess the efficacy of particular legal instruments in combating the financing of terrorism.

Although anti-terrorist financing law did not exist in 1985 when Air India Flight 182 was bombed, today's legal regime appears to be comprehensive. It is based primarily on two pieces of legislation examined here: first, the Criminal Code, and, second, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. These legislative initiatives cover significant regulatory ground in terms of substantive law, and, generally speaking, they also accord with private and public international law on terrorist financing.<sup>1</sup> The difficulty with the contemporary regime lies not in conspicuous gaps in the substantive law, but rather in knowing whether the regime is effective in fulfilling its stated objectives of preventing and disrupting the funding of terrorists.

This study focuses on the need to assess the current anti-terrorist financing regime and ensure that its infrastructure functions effectively. First, it suggests that a formal and full-fledged assessment of the efficacy of the current regime be undertaken. Second, it suggests that consideration be accorded as to whether a body that oversees and monitors the functions of FINTRAC should be created. Third, in the same vein, it suggests that study be undertaken on the issue of whether a larger oversight body is necessary, one that oversees not only the activities of FINTRAC, but also other institutions that bear responsibility for enforcing the terrorist financing laws, such as the RCMP and CSIS.

Thus, this study takes a pragmatic view of law. Law generally, and anti-terrorist financing law specifically, should not be viewed as a panacea

---

<sup>1</sup> The one area where this may not be true is in the area of reporting suspicious attempted transactions. However, the recommendations in Bill C-25 largely address this shortcoming. See Bill C-25, *An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the Income Tax Act and to make a Consequential Amendment to Another Act*, 1<sup>st</sup> Sess., 39<sup>th</sup> Parl., 2006, section 3(1)(g) [Bill C-25]. Bill C-25 received Royal Assent on December 14<sup>th</sup> and became S.C. 2006, c.12.

that can cure all political evils. Law is a tool, and, at times, a limited one. Unless we know whether current law is effective, we should not be keen to create additional legal requirements. This is because regulation is costly, and ineffective regulation imposes unnecessary costs.

Part 2 of this paper outlines the elements of the Canadian legal regime aimed at combating the financing of terrorist activities. Part 3 examines, on a comparative basis, the U.S. legal system regarding this subject to evaluate whether the Canadian regime is missing any important structural or legal elements. Part 4 contains the analysis central to this report including directions for future consideration and research. Part 5 concludes the discussion.

## 2. CANADIAN REGIME

The Canadian regime to counter the financing of terrorist activities has two main component parts: first, the amendments to the Criminal Code of Canada that deal with terrorist financing<sup>2</sup> and other related provisions in the Criminal Code<sup>3</sup>, and, second, Proceeds of Crime (Money Laundering) and Terrorist Act.<sup>4</sup> As these legal instruments were implemented within the past six years, they are ripe for evaluation, especially in light of claims that Canada is a “haven” for terrorists.<sup>5</sup> This section will examine these two layers of regulation.<sup>6</sup>

At the outset, it bears mentioning that Canada’s regime relating to the financing of terrorism appears to accord with international obligations. For example, Canada is a founding member of the Financial Action Task Force (FATF), an intergovernmental body of 33 countries that includes terrorist financing in its mandate. FATF has passed eight special recommendations on terrorist financing that have become international standards and that have provided a blueprint for the domestic law of its members. In addition, Resolution 1373 adopted by the UN Security Council in 2001

---

<sup>2</sup> R.S.C. 1985, c. C-46, sections 83.01-83.27 [*Criminal Code*].

<sup>3</sup> See e.g., *ibid.*, sections 462.32(4), 462.35 relating to the seizing of property and time periods under which property can be detained.

<sup>4</sup> S.C. 2000, c. 17 [*Proceeds of Crime Act or the Act*].

<sup>5</sup> U.S. Library of Congress, *Asian Organized Crime and Terrorist Activity in Canada*, (Washington, D.C.: Library of Congress 2003). See also “U.S. again brands Canada terrorist haven”, *The Globe and Mail* (15 February 2004).

<sup>6</sup> It should be noted that there are other aspects of the regulatory regime dealing with terrorism, as distinct from the financing of terrorism. These are usefully described in the recent Arar Inquiry Report. See Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP’s National Security Activities*, (Ottawa: Ministry of Public Works, 2006) c. 3 [*Arar Inquiry Report*].



states that countries shall “deny safe haven to those who finance, plan, support, or commit terrorist acts, or provide safe havens...”<sup>7</sup> It further states that countries shall “prevent those who finance, plan, facilitate, or commit terrorist acts from using their respective territories for those purposes...”<sup>8</sup> The Security Council Resolution does not provide guidance on structures that need to be established in order to effect these objectives. Nevertheless, as discussed here, Canada has abided by the Resolution in terms of the laws it has passed.

Implicit in this analysis is an understanding that terrorism, and the financing of terrorism, defies geographical boundaries.<sup>9</sup> A prime example is that money can be transferred without actually changing hands (for example, *via* an exchange of debt system).<sup>10</sup> Thus, an analysis of Canada’s laws is necessarily of limited use as questions persist regarding the extra territorial application of these laws. Two issues outside the mandate of this paper are significant here: whether the legislation at issue should be read to have extraterritorial effect; and, whether private and public international law permits Canada to apply its law to conduct in question.<sup>11</sup> Notably, however, the recent Criminal Code amendments discussed below may entail expanded jurisdiction to try offences committed outside of Canada if such offences would fall within the provisions of the Code.<sup>12</sup>

## Criminal Code

Section 83.01(1)(a)(x) of the Criminal Code defines “terrorist activities” as including acts committed outside or inside Canada that if committed in Canada would constitute an offence under section 83.02 in relation to providing or collecting property intending or knowing that it will be used for terrorism.<sup>13</sup> The list of what actions constitute a “terrorist activity” is lengthy, and includes conspiracy, attempt, or threat to commit listed acts

<sup>7</sup> *Charter of the United Nations*, SC Res. 1373(2001), UN SCOR, 2001, UN Doc. S/RES/1373 (2001), section 2(c).

<sup>8</sup> *Ibid.*, section 2(d).

<sup>9</sup> Walter Perkel, “Money Laundering and Terrorism: Informal Value Transfer Systems” (2003) 41 Am. Crim. L. Rev. 183-184.

<sup>10</sup> *Ibid.* at 188-189.

<sup>11</sup> *Supra* note 9 at 194-195 discussing extra-territoriality of U.S. law.

<sup>12</sup> See Criminal Code, *supra* note 2, section 7 (3.73) (extending jurisdiction to prosecute s., 83.02 offence committed outside of Canada in certain circumstances). See *supra* note 2, section 7 (3.74) (extending jurisdiction to prosecute other terrorism offences committed outside of Canada in certain circumstances).

<sup>13</sup> *Ibid.*, section 83.01(x) referring to subsection 7(3.73) that implemented the *International Convention for the Suppression of the Financing of Terrorism*, adopted by the General Assembly of the United Nations on December 9, 1999.

or omissions.<sup>14</sup> The first set of criminal offences is contained in sections 83.02-83.04, and consists of a three-pronged approach to counter terrorist financing. The offences are all indictable offences under which the accused is liable to imprisonment for a term of not more than ten years if convicted.

Specifically, section 83.02 of the Criminal Code imposes prohibitions on providing or collecting property to carry out terrorist activity. The provision applies to everyone who directly or indirectly “willfully and without lawful justification or excuse provides or collects property intending that it be used or knowing that it will be used” to carry out a terrorist activity has committed an offence under the Code. Although the prohibited act of this offence is defined quite broadly to the direct or indirect provision or collection of property, the offence has high fault requirements that require proof of an intent or knowledge that the property will be used for terrorism.

Section 83.03 creates an offence for anyone who directly or indirectly collects property, provides, or makes available property for terrorist purposes. The Code provides that no person shall knowingly deal in property that is owned or controlled by a terrorist group, or facilitate directly or indirectly any transaction in respect of such property. The prohibited act of this offence is also defined very broadly, and section 83.03(b) is quite broad because it applies to anyone who provides, or even invites a person to provide, property or financial or other related services knowing that will be used in whole or part to benefit a terrorist group. It is not necessary under section 83.03(b) to demonstrate any connection with any terrorist activity: “it is an offence merely to ‘use’ or ‘possess’ property with the intention or knowledge that it will be used for terrorist purposes”.<sup>15</sup>

Section 83.04 creates an offence for using or possessing property for terrorist purposes. In particular, anyone who “uses property, directly or indirectly, in whole or in part, for the purpose of facilitating or carrying out a terrorist activity” has violated the statute. Similarly, if a person possesses property and intends that it will be used, or knows that it will be used, to facilitate terrorist activity, they have violated the statute. This offence is

---

<sup>14</sup> *Ibid.*

<sup>15</sup> Kevin E. Davis, “The Financial War on Terrorism” in Victor V. Ramraj, Michael Hor, and Kent Roach, eds. *Global Anti-Terrorism Law and Policy* (Cambridge: Cambridge University Press, 2005) 182.

again worded broadly, but requires proof that the accused either has the purpose of facilitating or carrying out a terrorist activity, or intends or knows that it will be used for such purposes. The fault requirements of these various offences would have to be proven beyond a reasonable doubt.

In addition, under section 83.05(1), the Governor in Council may establish a list of entities that have knowingly carried out, facilitated, or attempted to carry out terrorist activities, or knowingly acted on behalf of terrorist entities. Once an entity is a listed entity, it will fall within the definition of “terrorist group” in section 83.01. A terrorist group is not, however, restricted to those entities, forty at present, that have been listed under section 83.05, and includes an entity that has as one of its purposes the facilitation or carrying out of terrorist activities, including an association of such entities.

A second set of offences relates to freezing and forfeiture of property. Under section 83.08, no person in Canada, or a Canadian outside of Canada, is permitted to deal with property knowing that it is controlled by a terrorist group, or provide financial or other related services for the benefit of a terrorist group. Furthermore, under section 83.1(1), every person in Canada, and every Canadian outside of Canada, must disclose to the RCMP and CSIS “the existence of property in their possession or control that they know is owned or controlled by, or on behalf of, a terrorist group”, as well as information about a transaction or proposed transaction in respect of such property.

Under section 83.11(1), certain listed financial institutions must determine on a continuing basis whether they are in possession or control of such property, and must make reports regarding the same on a monthly basis. Anyone who contravenes these offences is liable, on summary conviction, to a fine of \$100,000, or imprisonment for one year maximum, or both, or, if convicted on indictment, to imprisonment for a maximum of ten years. Unlike the offences under section 83.02-83.04, these offences are aimed primarily not at terrorists and their supporters, but to third parties who might deal with terrorist property. Such third parties may be more amenable to regulation; but, as discussed below, care should be taken not to impose unreasonable and costly burdens on them. Furthermore, section 83.09 contains an exemption scheme which allows the Solicitor General to provide an exemption from liability arising under one of the several provisions that prohibit the financing of terrorists.



In addition to these sections of the Criminal Code that deal specifically with financing of terrorism, Part XII.2 Proceeds of Crime addresses money laundering. If someone deals with property, or any proceeds of property, with the intent to conceal the property, and knowing or believing that all or part of the property was obtained from the commission or omission of a designated offence, she is liable to be convicted on either indictable offence or summary conviction.<sup>16</sup> Case law decided under the section suggests that past prosecutions have not involved terrorist activities per se, but to such things as drug trafficking<sup>17</sup> and, of course, money laundering alone.<sup>18</sup> Terrorism can be financed not only by money derived from crime, but also by money derived from other sources, including legitimate earnings, and funds given to charities.

The money laundering provisions are extremely broad and deal with “property or proceeds obtained directly or indirectly”. Strictly interpreted, these provisions contain a broad *actus reus*. The New Brunswick Court of Appeal has held (affirming a decision at first instance) that in order for property to be included as proceeds of crime, the property must be directly linked to the commission of the criminal act in question.<sup>19</sup> Establishing the *mens rea* requirement is also potentially problematic, since the accused must “know or believe all or some [of the property or proceeds] was obtained directly or indirectly...” Again, this is an extremely broad phrase, and suggests that “almost any connection with criminal activity will be caught by this section.”<sup>20</sup>

As will be noted below, there is some overlap between the obligations in the Criminal Code and those contained in the Proceeds of Crime Act which raises the question of whether this area of law is “overregulated”. First, they both contain provisions that aim to address money laundering. Second, they both contain reporting requirements. The Criminal Code requires that every person in Canada, and every Canadian outside of Canada, disclose information about a transaction, or proposed transaction, in respect of property owned or controlled by, or on behalf of, a terrorist group. Similarly, the Proceeds of Crime Act contains reporting requirements that apply to a list of entities that closely resembles the list contained in the Criminal Code. Third, they both have provisions relating

---

<sup>16</sup> Criminal Code, *supra* note 2, sections 462.31(1), 462.31(2).

<sup>17</sup> See e.g. *Giles v. Canada* [1991] 63 C.C.C. (3d) 184.

<sup>18</sup> *R. v. Hape* [2000] 148 C.C.C. (3d) 530.

<sup>19</sup> *R. v. Shalala* (1998), 198 N.B.R. (2d) 298, *aff'd* [2000] N.B.R. (2d) 118. See also David Samuel-Strausz Vernon, “A Partnership with Evil: Money Laundering, Terrorist Financing and Canadian Financial Institutions” (2004) 20 B.F.L.R. 89 at 94.

<sup>20</sup> Laundering Database (May 1, 1998) at para 8 online [www.quicklaw.com](http://www.quicklaw.com).



to the compilation of a list of terrorist entities; and they both seek to target entities that “facilitate” the financing of terrorist activities.

While overlap between criminal and regulatory offences is common, one of the functional problems of overlap is the existence of different, and possibly uncoordinated, enforcement regimes. In particular, prosecution of terrorist offences under the Criminal Code must be pre-approved by the provincial or federal Attorney General. But, who enforces the Proceeds of Crime reporting requirements (FINTRAC and/or police authorities); and, is there a need for co-ordination between the enforcement authorities?

### **Proceeds of Crime Act**

While the Criminal Code addresses a variety of activities that relate to terrorist financing (from providing property, to assist in terrorist financing, to money laundering) and criminalizes such activity, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act deals with reporting requirements, cross-border movement of currency, and the creation of an agency to administer the Act.

Under section 7 of the Act, defined individuals and entities report transactions “in respect of which there are reasonable grounds to suspect that the transaction is related to the commission of...a terrorist activity financing offence.”<sup>21</sup> In addition, if these individuals and entities are required to make a report under section 83.1 of the Criminal Code, they must also make the report to the agency that is responsible for administering the Proceeds of Crime Act: the Financial Transactions and Reports Analysis Centre (FINTRAC).<sup>22</sup> FINTRAC’s purpose is to facilitate the detection, prevention, and deterrence of money laundering and the financing of terrorist activities. FINTRAC also has the authority to receive voluntary information from various sectors of the public, including law enforcement agencies, about suspicions of terrorist financing.<sup>23</sup>

The fact that reports must go to FINTRAC and, under the Criminal Code, to the heads of the RCMP and CSIS, suggests that the legislation creates a system, perhaps for privacy reasons, in which agencies do not share information. While information sharing may be beneficial for efficiency and

---

<sup>21</sup> *Proceeds of Crime Act*, *supra* note 4, section 7.

<sup>22</sup> *Ibid.*, section 7.1(1).

<sup>23</sup> *Ibid.*, section 7.1.

efficacy reasons, Posner has argued that post-9/11, the U.S. government chose reforms that result in a top-heavy and overly centralized intelligence system. Posner argues that in intelligence generally, it is best to have multiple centers, as centralization can be ineffective.<sup>24</sup> This is a point that will be discussed further below.

Every person or entity that breaches the reporting requirements contained in the Act is liable on summary conviction to a \$500,000 fine or 6 months in prison or both for first time offences. For subsequent offences, the fine is increased to \$1,000,000 and the prison term is one year or both; or, on conviction on indictment, to a \$2,000,000 fine or 5 years in prison or both. Thus, for failing to report, persons or entities face significant penalties. It is not clear on the face of the statute which body enforces contravention of the Act when these offences occur.

The Act contains a defence for employees in respect of transactions that they reported to their superiors.<sup>25</sup> However, directors and officers are guilty of an offence if they direct, authorize, assent to, acquiesce in, or participate in an act that violates the statute.<sup>26</sup> These individuals do have a defence available if they establish that they exercised due diligence to prevent the commission of the act.<sup>27</sup> However, the liability of directors and officers under the statute appears to be a regulatory offence.

In addition to the reporting requirement on individuals and entities, persons arriving in or leaving Canada must file reports regarding the importation and exportation of currency or monetary instruments over a prescribed amount.<sup>28</sup> Customs officers may retain currency and monetary instruments at the border, and these are forfeited to the federal government.<sup>29</sup> Officers may search these individuals,<sup>30</sup> conveyances,<sup>31</sup> and baggage,<sup>32</sup> as well as any mail being imported or exported.<sup>33</sup>

Under the Act, the persons and entities that have reporting and monitoring functions to FINTRAC under section 7 include: authorized

---

<sup>24</sup> Richard A. Posner, *Uncertain Shield: The U.S. Intelligence System in the Throes of Reform* (Lanham: Rowman & Littlefield, 2006).

<sup>25</sup> *Proceeds of Crime Act*, *supra* note 5, section 75(1).

<sup>26</sup> *supra* note 5

<sup>27</sup> *Ibid.*, section 79(b).

<sup>28</sup> *Ibid.*, section 12(1), 12(3).

<sup>29</sup> *Ibid.*, section 14(5).

<sup>30</sup> *Ibid.*, section 15(1).

<sup>31</sup> *Ibid.*, section 16(1).

<sup>32</sup> *Ibid.*, section 16(2).

<sup>33</sup> *Ibid.*, section 17(1).

banks, cooperative credit societies, loan and trust companies, portfolio managers, securities dealers, casinos, and various other business entities.<sup>34</sup> Amendments to the Act contained in Bill C-25 broaden the persons and entities required to engage in record-keeping and reporting of activities; this list now includes businesses that deal in securities or any other financial instruments, for example.<sup>35</sup> However, even with these amendments, there are undoubtedly organizations and less formal institutions (such as “hawals”, informal trust-based systems for transferring funds<sup>36</sup>) that are not subject to reporting obligations under the statutory schema. Simply because the breadth of the list has been expanded under Bill C-25 does not mean that such organizations will be caught by its terms.

Bill C-25 also attempts to deal with the issue of funds channeled through charitable organizations. The Bill amends the Income Tax Act to allow the Canada Revenue Agency (CRA) to disclose to FINTRAC, the RCMP, or CSIS information about charities suspected of being involved in terrorist financing activities.<sup>37</sup> It appears from the legislation that the CRA is able to choose the entity to which it provides information.<sup>38</sup> The Bill C-25 amendments to the Income Tax Act also permit information sharing among CSIS and the RCMP for purposes of investigating whether an offence may have been committed, or whether certain activities constitute securities threats. But there is no requirement for information sharing, and certainly no oversight body that monitors the conduct of these organizations when they act pursuant to the legislation.

Common law has established that there is a duty of secrecy and confidentiality on bankers in their relationships with customers. In *Tournier v National Provincial & Union Bank of England*, the English Court of Appeal held that the bank is the custodian of its customers' confidential information and has a duty not to disclose such information.<sup>39</sup> However, the case also isolated certain exceptions to the rule, including where there is a duty to the public to disclose, or where the interests of the bank require disclosure. Thus, it could certainly be argued on either of these grounds that where a terrorist organization is utilizing a bank for the funneling of illegal funds contrary to the law of Canada, it is in the public

---

<sup>34</sup> *Ibid.*, section 5.

<sup>35</sup> *Bill C-25*, *supra* note 1.

<sup>36</sup> U.S., National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, D.C.: United States Government Printing Office, 2004) at 171.

<sup>37</sup> *supra* note 2

<sup>38</sup> *Ibid.*

<sup>39</sup> (1923), [1924] 1 K.B. 461 (C.A.).

interest, as well as the bank's own interest, to disclose these transactions.<sup>40</sup> Furthermore, there are certain legislative provisions that protect banks and others from civil claims.<sup>41</sup>

The proposed amendments in Bill C-25 also broaden the scope of the reporting obligation. Whereas the current Act requires reporting of every financial transaction that *occurs* and is related to the commission of a terrorist activity financing offence, the amendments deal with "every financial transaction that occurs or that is *attempted*...and in respect of which there are reasonable grounds to suspect that:...(b) the transaction is related to the commission *or the attempted commission* of a terrorist activity financing offence."<sup>42</sup> In addition, the Bill adds a new prohibition to the Act which prohibits persons from opening an account on behalf of the person if it cannot establish his or her identity.<sup>43</sup> These persons must also determine whether they are dealing with a "politically exposed foreign person"<sup>44</sup> and, if so, they must obtain the approval of senior management before proceeding.<sup>45</sup> Numerous measures must be adopted before an entity enters into a banking relationship with a foreign entity.<sup>46</sup>

FINTRAC is in many senses a gatekeeper of information. It receives information from three bodies: federal agencies such as CSIS and the RCMP, foreign intelligence bodies and, of course, reports regarding suspicious transactions from the private sector.<sup>47</sup> FINTRAC also makes decisions regarding where to channel this information, if anywhere. If it has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting terrorist activity, FINTRAC must disclose the information to the appropriate police force, Revenue Canada, and the Canada Border Services Agency.<sup>48</sup> It is required to

---

<sup>40</sup> However, it should be noted first that such a breach of confidentiality is likely in advance of any hard proof that the laws of Canada have been broken. Thus, it would not be clear if the public interest were indubitably at risk. Furthermore, laws that compel disclosure of customers' information run the risk of invading their privacy, an issue discussed in greater detail below.

<sup>41</sup> See Criminal Code, *supra* note 3, section 83.1(2) which states that "No criminal or civil proceedings lie against a person for disclosure made in good faith under subsection (1)".

<sup>42</sup> *supra* note 3

<sup>43</sup> *supra* note 2

<sup>44</sup> This term is defined as a "person who holds or has held one of the following offices or positions in or on behalf of a foreign state", and includes a list consisting of a number of officials including: head of state or head of government, deputy minister, ambassador, head of government agency, judge...

See Bill C-25, *supra* note 2, section 8.

<sup>45</sup> *supra* note 2

<sup>46</sup> *Ibid.*

<sup>47</sup> See *Arar Inquiry Report*, *supra* note 7 at 567.

<sup>48</sup> *supra* note 7



disclose information to CSIS if it “has reasonable grounds to suspect that designated information would be relevant to threats to the security of Canada.”<sup>49</sup>

The term “designated information” means, in respect of a financial transaction, the name of the client, the name and address of the place where the transaction occurred, the amount and type of currency involved, the transaction number and the account number, and any other identifying information that may be prescribed.<sup>50</sup> FINTRAC may also disclose designated information to an institution or agency of another country or an international organization.<sup>51</sup> However, FINTRAC may not disclose any information that would serve to identify an individual who provided information to it<sup>52</sup>, and cannot disclose information provided to it in regards of suspicious transactions. FINTRAC is required, however, to disclose information if it determines that there are reasonable grounds to suspect that the information would be relevant to investigating a terrorist financing or money laundering offence.<sup>53</sup>

Not contained in the legislative schema is a list of the criteria to be applied by FINTRAC in making a decision regarding whether to provide information to CSIS and/or the RCMP. However, FINTRAC’s 2006 Annual Report states:

Once we determine that there are reasonable grounds to suspect that the information would be relevant to the investigation or prosecution of a money laundering and/or terrorist activity financing offence and/or threats to the security of Canada, FINTRAC must disclose “designated information” to the appropriate police force or to CSIS.<sup>54</sup>

---

49 *supra* note 5

50 *supra* note 5

51 *Ibid.*, sections 56.1(1)-(2).

52 *Ibid.*, section 58(2).

53 *Ibid.*, sections 55(1), 55(3).

54 Canada, *FINTRAC 2006 Annual Report*, (Ottawa: FINTRAC, 2006), online: FINTRAC <[http://www.fintrac.gc.ca/publications/annualreport/2006/3\\_e.asp](http://www.fintrac.gc.ca/publications/annualreport/2006/3_e.asp)> [Annual Report].

FINTRAC thus holds discretion in terms of funnelling information to the RCMP and CSIS. It is not clear from the legislation whether FINTRAC would be justified in providing information to one of these entities alone. Furthermore, to what extent does FINTRAC coordinate efforts with these institutions? If these entities do share information, what is the nature of information sharing among them? For purposes of both efficiency and efficacy, this is a crucial practical consideration distinct from the precise legal provisions outlined above. In creating FINTRAC, a body that operates alongside but not necessarily in cooperation with CSIS and the RCMP, the *Proceeds of Crime Act* may contribute to an overall problem of inefficacy. FINTRAC's effectiveness will be affected by the degree of co-operation and information sharing between the RCMP and CSIS.

### 3. UNITED STATES

This section examines the main U.S. legislative provisions governing the financing of terrorism. These are the U.S. Criminal Code, the Patriot Act, the 1956 and 1957 money laundering statutes, and the Bank Secrecy Act. It will engage a comparison between Canadian and U.S. law and examine a key institutional structure present in the U.S. but not in Canada: the U.S. Office of Terrorism and Financial Intelligence.

#### U.S. Criminal Code

The U.S. Criminal Code contains a crime of terrorist financing which has been in place since 1994. The particular offense, contained in section 2339A, is entitled "Providing material support to terrorists", and reads as follows: "whoever ... provides material support or resources or conceals or disguises the nature, location, source, or ownership of material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out, a violation of [terrorist financing]... shall be fined... imprisoned not more than 15 years, or both, and if the death of any person results, shall be imprisoned for any term of years or for life..."<sup>55</sup>

The words "terrorist financing" are not contained in the section but the section includes by reference crimes listed in 18 USC 2332B dealing with violent crimes including "federal crimes of terrorism". Based on these provisions, the Department of Justice has stated that the term "terrorist financing" refers to the act of knowingly providing something of value

---

<sup>55</sup> 18 U.S.C. para 2339A.

to persons and groups engaged in terrorist activity.<sup>56</sup> The term “material support or resources” is defined in section 2339A and includes “currency or monetary instruments or financial securities, financial services...” A similar offence, contained in section 2339B, exists for providing material to a foreign terrorist organization.<sup>57</sup>

There are two Executive Orders also relevant to terrorist financial networks. First is Executive Order 13224 entitled “Blocking Terrorist Property”. This Order expands the U.S. Treasury’s authority to freeze assets and U.S. transactions of persons or institutions associated with terrorists and terrorist organizations.<sup>58</sup> The Treasury can also freeze the assets of, and deny U.S. access to, foreign banks that refuse to cooperate. Second is Executive Order 13382, entitled “Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters”. It provides the U.S. Treasury with authority aimed at freezing the assets of proliferators of weapons of mass destruction (WMD) and their supporters.<sup>59</sup>

As the Department of Justice has stated, the philosophical underpinning of the U.S. strategy since 9/11 has been “strategic overinclusiveness”. It was felt that even humanitarian and charitable organizations will need to come within the law and a broad-based legal approach (further set out below) would be necessary to ensure this occurred. Finally, the U.S. did not want to have to trace moneys from the U.S. to their ultimate use.<sup>60</sup>

## Patriot Act

The U.S. Patriot Act<sup>61</sup> provides federal officials with authority to track and intercept communications, and the Secretary of the Treasury with a legislative arsenal to combat corruption of U.S. financial institutions for foreign money laundering purposes. The Patriot Act contains a focus on banks as a conduit of money laundering by “hiding the identity of real parties in interest to financial transactions...”<sup>62</sup> The Act is also concerned with foreign government bodies as being potentially corrupt “particularly

<sup>56</sup> 18 U.S.C. para 2339A. See also U.S. Department of Justice, “Terrorist Financing” (2003) Vol 51:4 [http://www.usdoj.gov/usao/eousa/foia\\_reading\\_room/usab5104.pdf](http://www.usdoj.gov/usao/eousa/foia_reading_room/usab5104.pdf) [DOJ publication].

<sup>57</sup> 18 U.S.C. para 2339B.

<sup>58</sup> Executive Order 13224 of September 23, 2001 “Blocking Terrorist Property” <http://www.state.gov/sct/rls/fs/2002/16181.htm>.

<sup>59</sup> Executive Order 13382 of June 28, 2005 “Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters” <http://www.fas.org/irp/offdocs/eo/eo-13382.htm>.

<sup>60</sup> DOJ publication, *supra* note at 8-9.

<sup>61</sup> USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 [Patriot Act].

<sup>62</sup> Patriot Act, *ibid.*, section 302(6).

if those services include the creation of offshore accounts and facilities for large personal funds transfers to channel funds into accounts around the globe.”<sup>63</sup>

Specifically under the Act, all financial institutions must create anti-money laundering programs. Treasury has the authority to impose information-gathering measures on business sectors that do not adhere to anti-money laundering standards imposed by regulators. The legislation appears more directly to regulate the private sector than does Canada’s which simply imposes duties, the violation of which can result in criminal or regulatory prosecutions. Treasury has the authority to facilitate the sharing of suspicious activity reports with other countries, specifically, the intelligence communities in these countries. Measures exist to prevent individuals from purchasing financial anonymity, for example, through shell banks with no physical presence.<sup>64</sup>

The Patriot Act is balanced, because it ensures that any forfeitures made in connection with anti-terrorist efforts permits “for adequate challenge consistent with providing due process rights...”<sup>65</sup> The Canadian forfeiture provisions contemplate notice to those who are known to own or control property subject to forfeiture, some protections for innocent third parties who have exercised reasonable care to ensure that the property would not be used for terrorist purposes and appeals to the Federal Court of Appeal.<sup>66</sup>

The Patriot Act seeks to strengthen the ability of banks and other financial institutions to maintain the integrity of their employee population...”<sup>67</sup> Notably, there is recognition that cooperative efforts are necessary between private and public sector. The Act explicitly provides for cooperation among financial institutions, regulatory authorities, and law enforcement authorities on matters relating to financing of terrorist groups<sup>68</sup>, including through the use of charities, nonprofits, and nongovernmental organizations.

---

<sup>63</sup> *Ibid.*, section 302(7).

<sup>64</sup> Mariano-Florentino Cuellar, “The Tenuous Relationship Between The Fight Against Money Laundering and the Disruption of Criminal Finance” (2003) 93 J. Crim. L. & Criminology 311 at 362.

<sup>65</sup> *Patriot Act*, *supra* note 62, section 302(8).

<sup>66</sup> *supra* note 62

<sup>67</sup> *supra* note 3

<sup>68</sup> *Ibid.*, section 314(a)(2)(A).



It is not clear that the Canadian regime adequately addresses information sharing among governments as the U.S. clearly attempts to do with these legislative provisions.<sup>69</sup> However, information sharing, especially among governments and agencies at an international level, may undermine domestic prosecutions in Canada. This is especially the case if Canadian officials have received information from foreign agencies, and would be forced to disclose such information if they pursued the prosecution. Revealing such information may impede law enforcement activities in the foreign jurisdiction, and may strain relations with the foreign agency so as to undermine or sever the relationship that led to the information sharing in the first place.

Furthermore, although Canada has various layers of terrorist financing legislation in place, there is no apparent legal requirement that institutions and regulators operate in tandem or via joint efforts. While this cooperation may exist in practice, there would be undoubted benefits in discerning the extent of any existing cooperation (such as in the area of information sharing), and perhaps mandating such cooperation in law. As argued below, consideration should be given to whether there should be some sort of oversight of government's regulation of the private sector.

## Money Laundering Statutes

Together with the registration and reporting requirements under the Patriot Act, the main pieces of legislation used to punish those who finance terrorism are two legislative provisions relating to money laundering.<sup>70</sup> Specifically, Section 1956 (referred to as the 1956 money laundering statute) criminalizes concealing criminal proceeds and promoting certain types of criminal conduct with monetary proceeds. Thus, if a person attempts or actually conducts a financial transaction that involves proceeds of a specified unlawful activity, and knows that the property involves proceeds of crime, this person will violate Section 1956(a)(1). Thus, the elements of the offence include: knowledge; existence of proceeds derived from unlawful activity; financial transaction; and, intent.<sup>71</sup> The Patriot Act expanded the category of specified unlawful

<sup>69</sup> Canada, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (Ottawa: Ministry of Public Works, 2006) at 331 [Arar Events Report]. While the Report does not engage in a U.S.-Canada comparative analysis on this issue, it does note that information sharing, done in a responsible manner, is vital, and recommended that the RCMP maintain and follow policies relating to information sharing. This issue is addressed *infra* section 4.

<sup>70</sup> *Laundering of Monetary Instruments*, 18 U.S.C. section 1956 (1986).

<sup>71</sup> See e.g. *United States v Sayakhom* 186 F.3d 928 at 942-43. See also Cuellar *supra* note 65 at 337-338.

activity that includes a list of “terrorism offences”<sup>72</sup> which includes financial transactions.<sup>73</sup> Section 1956(a)(2) also creates a separate crime targeting the international movement of money connected with some crimes.

Section 1957 targets conduct involving transactions with certain types of criminal proceeds. The section prohibits knowingly disbursing or receiving more than \$10,000 of criminally derived proceeds if a financial institution is utilized. The elements of the offences are: (a) engaging or attempting to engage; (b) in a monetary transaction (which is defined to mean the use of a financial institution); (c) in criminally derived property; (d) valued at more than \$10,000; (e) the property derives from specified unlawful activity (as defined under Section 1956); and, (f) the person knows that the property is criminally derived.<sup>74</sup>

We should note limits of this legislation and terrorist financing laws generally. In particular, acts of terrorism may be financed with funds that do not derive from criminal sources. The 9/11 Commission Report concluded that “it cost al Qaeda about \$30 million per year to sustain its activities before 9/11 and...this money was raised almost entirely through donations.”<sup>75</sup> The Report further concluded that al Qaeda had numerous sources of funding, and the authors of the report found no evidence that any person in the U.S., any foreign government, or foreign government official provided financial assistance to the hijackers.<sup>76</sup> The difficulty in finding evidence is not limited to the 9/11 attacks, but is likely pervasive in this area of law. It is not unreasonable to question, therefore, whether terrorist financing legislation is effective in preventing and combating terrorist activity.

## The Bank Secrecy Act

The U.S. also has in play a system of regulatory rules and procedures aimed specifically at financial institutions. The main purpose of these rules is to create a reporting procedure to obtain information about suspicious transactions, and to provide for sanctions in the case of violating reporting procedures. Administered by the U.S. Treasury, the Bank Secrecy Act (formally the Currency and Foreign Transactions Reporting

---

<sup>72</sup> *Supra* note 62

<sup>73</sup> See 18 U.S.C. section 2332d (1996).

<sup>74</sup> For discussion, see Cuellar *supra* note 65 at 342.

<sup>75</sup> *Supra* note 65

<sup>76</sup> *Supra* note 37.

Act)<sup>77</sup> contains a long list of institutions subject to the Act, including: state chartered commercial banks, post offices, casinos, and securities firms. It also provides discretion to the U.S. Treasury Department to define further the term “financial institutions”.

Entities that fall within this definition must report any single currency transactions over \$10,000, and multiple transactions over this amount that are conducted on the same day (if the institution knows that the transaction was conducted on behalf of the same person).

This reporting procedure resembles to some extent the process laid out in the current Proceeds of Crime Act but includes a broader list of obligated entities. Bill C-25 is more closely aligned with this U.S. statute, especially in its extension of the list of entities caught by the reporting obligation. However, Bill C-25 does not allow government agencies to define further the list of regulated entities and in this way is not as broad as the U.S. law.

## Office of Terrorism and Financial Intelligence

Created in 2004, the U.S. Office of Terrorism and Financial Intelligence (OTFI) is a division of Treasury that consolidates the policy, enforcement, regulatory and international functions of the Treasury in the area of terrorist financing. The OTFI aims to detect the exploitation of financial systems by terrorists. It also allows implementation of regulatory enforcement programs (including sanctions) as well as cooperation with the private sector and international bodies against terrorist financing.<sup>78</sup>

The OTFI has as its main objective gathering and analyzing information from the intelligence, law enforcement, and financial communities regarding means by which terrorists earn, move, and store money. It has the ability to adopt policy, regulatory or enforcement actions to freeze assets of terrorists, prevent corrupt financial institutions from operating in the U.S. and trace and repatriate assets looted by corrupt foreign officials.<sup>79</sup> The OTFI advises the government in areas of combating rogue financial threats, including terrorism and weapons of mass destruction

<sup>77</sup> P.L. 91-508, Titles I and II, as amended, codified at 12 USC 1829b – 1951059 (2000) and 31 USC 5311-5330 (2000). See also 31 C.F.R. section 103 (2002). See Cuellar, *supra* note 65 at 351-352 for discussion.

<sup>78</sup> *Supra* note 65

<sup>79</sup> United States Department of the Treasury, “Terrorism and Financial Intelligence Goals”, United States Department of the Treasury <<http://www.treasury.gov/offices/enforcement/goals.shtml>>.

proliferation financing, money laundering and other financial crimes.<sup>80</sup> The Department of Treasury submits an annual Performance and Accountability Report to Congress. Contained in this report is a summary of the activities of the OTFI and other aspects of Treasury's efforts to combat the financing of terrorism (including a description of its activities relating to the administration of the Bank Secrecy Act).

Canada does not have a coordinating body of this nature and certainly does not have the many layers of infrastructure that the U.S. has in the area of anti-terrorist financing. While inefficiencies can emerge from centralization of this nature (per Posner discussed above), the question arises as to whether some type of body that coordinates would serve a useful function. In particular, it would be useful to contemplate the benefits of a body that oversees the efforts of the individual entities that play a role in curbing and monitoring terrorist financing. Such a body could, as in the United States, report to the legislature or legislative committees that could conduct a review of the effectiveness of regulation and the co-ordination of regulatory efforts.

## 4. ANALYSIS

### A. Problems with Current Regime

Before we evaluate whether reforms to the current regime are necessary, we must understand problems underlying the regime. In this section, we turn to examine some of these issues relating to: efficacy of the current legal regime; information sharing; privacy rights; costs on private institutions; and, charities.

*Efficacy.* The Proceeds of Crime Act is, to a great degree, focused on private (as opposed to governmental) actors and compels them to undertake reporting and monitoring of suspicious transactions. The Act together with the amendments contained in Bill C-25 contain broad reporting obligations that apply to every financial transaction where there are reasonable grounds to suspect that the transaction is related to the "commission or attempted commission of a terrorist activity financing offence".<sup>81</sup> Thus, the obligation to report applies if such transaction

---

<sup>80</sup> See United States Department of the Treasury, "Education Duties & Functions", online: United States Department of the Treasury < <http://www.treas.gov/education/duties/treas/u-sec-enforcement.shtml> >.

<sup>81</sup> *Bill C-25, supra* note 2, section 5.



occurs or if the transaction is merely attempted. The provisions seem so broad that they conceivably capture any number of interchanges. A host of questions arise: Is it reasonable to expect that financial institutions will report all such interchanges? Is creating a statutory offence the best or only way to encourage the reporting? Should we devote resources to improving the capacity of financial institutions to spot suspicious transactions? How much of the financing of terrorist activities occur through the financial institutions subject to reporting requirements?

FINTRAC's Annual Report for 2005-06 states its results according to "case disclosures" each of which consists of a bundle of "designated information" about the individual or company involved in reportable transactions.<sup>82</sup> In its Report, FINTRAC states that 168 case disclosures were made: 134 of these were for suspected money laundering while 33 were for "suspected terrorist activity financing and/or other threats to the security of Canada". One case disclosure involved both of these items.<sup>83</sup> The Annual Report does not indicate to whom the case disclosures were made, only that the designated information must be disclosed to the appropriate police force or CSIS, as well as to the Canada Revenue Agency and the Canada Border Services Agency.<sup>84</sup>

The Annual Report also states that FINTRAC has improved the "sophistication and thoroughness of our analytical process" and has received a growing amount of information "from law enforcement and national security agencies."<sup>85</sup> The Report states that "Canadian financial institutions and other financial intermediaries are becoming more effective in detecting suspicious transactions."<sup>86</sup> The number of suspicious transaction reports is stated to have increased from 19,111 in 2004-05 to 29,367 in 2005-06.

Thus, in total there were 33 case disclosures on terrorism financing from almost 30,000 reports from financial institutions (.0011%). Despite the voluminous paperwork filed and received by FINTRAC, the result appears to be that only a minimal amount of disclosures relate to suspicious transactions. In addition, one must question what happens with these

---

<sup>82</sup> *Supra* note 2

<sup>83</sup> *Supra* note 55

<sup>84</sup> *Ibid.* at 5.

<sup>85</sup> *Ibid.* at 9.

<sup>86</sup> *Ibid.* at 9.

33 disclosures. No pure financing prosecutions have been launched.<sup>87</sup> In short, given that the legislative system is based on information flows in and out of FINTRAC, it is imperative to know what happens with the information.

The mere fact that entities such as banks and other financial institutions report frequently does not indicate whether those entities that most need to report are in fact doing so or that the information that is being reported is in fact of significance. In order to determine whether the reporting mechanism is effective in weeding out suspicious transactions, we need to know whether the transactions were legitimately and actually “suspicious”. The fact that they were reported does not make them so. The reality is that from these results it is unclear how effective FINTRAC has been in fulfilling its mandate to facilitate the detection, prevention and deterrence of money laundering and the financing of terrorist activities.<sup>88</sup> The case disclosures and information regarding suspicious transactions tell us nothing about whether an actual threat was curtailed. Were these cases resolved? Were these transactions legitimately labeled “suspicious”? While the information that FINTRAC receives may assist in detecting the targeted activities, there is nothing to indicate that FINTRAC has been successful in its deterrence role.<sup>89</sup>

The recent Senate Banking, Trade and Commerce Committee suggests that FINTRAC’s numbers may be low. In a report issued in 2006, the Senate Committee concluded that the amount of dirty money laundered in Canada each year by criminals and terrorists “is probably in the tens of billions of dollars”.<sup>90</sup> However, the Senate Committee completed no statistical examination of costs and benefits but focused instead on anecdotal reports from, and interviews with, various industry actors. The point remains, therefore, that until this time, there has been no concerted and comprehensive effort towards determining whether the current legislative regime is effective in preventing terrorism and the costs and benefits inherent in the regime.

---

<sup>87</sup> Yet this does not necessarily mean that the 33 disclosures were ineffective in terms of disruption and surveillance. Reference is made to the case of *R. v. Khawaja* involving a section 83.03 charge of Mohammad Momin Khawaja who was arrested March 29, 2004 and accused of participating in the activities of a terrorist group, and facilitating a terrorist activity. See *R. v. Khawaja* [2006] O.J. No. 4245.

<sup>88</sup> See *Annual Report*, *supra* note 55.

<sup>89</sup> *Supra* note 55

<sup>90</sup> Canada, Standing Senate Committee on Banking, Trade and Commerce, *Stemming the Flow of Illicit Money: A Priority for Canada*, (Ottawa: The Senate of Canada, 2006) at 1, online: Parliament of Canada < <http://www.parl.gc.ca/39/1/parlbus/commbus/senate/com-e/bank-e/rep-e/rep09oct06-e.pdf> > [*Senate Committee Report*].

*Information Sharing.* This issue has two aspects: first, inter-agency information sharing and, second, sharing between FINTRAC and entities that file reports with it. FINTRAC is the repository of a great amount of information relating to suspicious transactions. This includes reports of suspicious transactions from CSIS and the RCMP, as well as reports from customs officers and the Canada Revenue Agency (under Bill C-25). To what extent are these channels being utilized? Is there information sharing among agencies? If the RCMP is undertaking an investigation, to what extent will FINTRAC share information that may be relevant to the RCMP investigation? In what circumstances does FINTRAC pass information to CSIS and in what circumstances does it pass information to the RCMP? Do the RCMP and CSIS share the information that is passed on and do they co-ordinate their efforts with respect to terrorism financing? These issues require evaluation.

FINTRAC also receives information from financial institutions subject to the Proceeds of Crime Act. Under the current system, if one bank has reported suspicious activities, it likely does not know of possible similar suspicious activities by the same perpetrator at another bank that has also reported. It also may have no idea of whether any of the reports it filed with FINTRAC concerned entities that it needs to monitor going forward. This information sharing among institutions that are subject to the Proceeds of Crime Act would perhaps better enable them to carry out what is primarily a monitoring function (that seems to be overshadowed by a reporting obligation). At the very least it would make sense to have a system of “alerts” that FINTRAC provides to all financial entities once it receives suspicious reports upon which it (or other law enforcement channels) has acted.

The Senate Committee raised similar concerns in its recent report. The Committee contemplated that the legal regime may be more effective if there were a two-way flow of information between FINTRAC and law enforcement and intelligence agencies as well as between FINTRAC and the financial entities that report to it. The Senate Committee concluded, “more information shared among the parties would result in more effective detection and deterrence.”<sup>91</sup> Representing certain financial entities, the Canadian Bankers’ Association suggested to the Senate Committee that more feedback from FINTRAC would be useful in developing its reporting mechanisms.<sup>92</sup>

---

91 Senate Committee Report, *ibid.* at 16.

92 See *ibid.* citing comments from the Canadian Bankers’ Association.



The main difficulty with information sharing, of course, is possible infringement of privacy rights as discussed below. Furthermore, even with a two-way flow of information, it is not clear whether such open channels prevent terrorist financing or assist in doing so. Even if some forms of terrorism financing are stopped, it is possible that terrorists will find other means to finance their activities.

*Privacy Rights.* Under the Proceeds of Crime Act, there is a prohibition on officials (of FINTRAC) to refrain from disclosing certain information contained in reports that are submitted or other information obtained under the Act.<sup>93</sup> However, this information may be disclosed where officers have reasonable grounds to suspect that the information “would be relevant to investigating or prosecuting...a terrorist activity financing offence.”<sup>94</sup> This means that whenever an officer on reasonable basis suspects information to be relevant in an investigation, this information can be disclosed. Questions arise as to what constitutes “reasonable grounds”. The Act and its proposed amendments do not provide guidance on what types of information are to be collected and what is the threshold for disclosure of collected information in the context of an investigation.

In terms of the entities that report under the Proceeds of Crime Act, the threshold for determining whether information should be reported is low and continues to decrease under Bill C-25. Listed entities must report every financial transaction that occurs or that is attempted. This means that the broad group of persons and entities caught by the reporting provision will be reporting transactions that provide reasonable grounds to suspect a terrorist financing activity, but which are not necessarily terrorist financing activities. In other words, a great many transactions may be reported that have no connection at all to terrorist financing. The concern is that otherwise private information is made public; and, more particularly, the private information of innocent customers is disclosed to FINTRAC, and possibly by FINTRAC if it passes on information to CSIS or the RCMP.

There has been criticism regarding the invasion of privacy brought about by the Proceeds of Crime Act, including the proposed amendments to the Act. The privacy concerns become even greater when we recognize that the Proceeds of Crime Act takes a broad-brush approach that results in many innocent transactions being reported. Some have suggested

---

<sup>93</sup> *Proceeds of Crime Act*, *supra* note 5, section 36(1).

<sup>94</sup> *Supra* note 5



creating an independent review commission with the powers and authority to conduct random reviews of FINTRAC's files and operations. Indeed, the Arar Commission recommended that the Security Intelligence Review Committee (SIRC) be given jurisdiction to review the national security activities of FINTRAC.<sup>95</sup> Administrative burdens and increasing expenses may weigh against the creation of such an agency. However, a strong case can be made that under the Act, intrusions into the affairs of individuals and businesses alike are extensive. The Senate Committee raised a similar point in its recent report, asserting that any legislative changes to the Proceeds of Crime Act must be considered with due regard to safeguarding the balance between the need for information that is reported on the one hand and the privacy of Canadians on the other.<sup>96</sup>

**Costs.** The private sector bears much, if not most, of the burden of in the legislative amendments designed to prevent financing of terrorists.<sup>97</sup> As discussed above, the main targets of reporting requirements under both Canadian and U.S. legislation are financial institutions. The Economist discusses compliance costs of this type of legislation in the UK context:

The compliance costs for financial institutions are substantial. Graham Dillon of KPMG, a consultancy, reckons it costs each mid-tier bank in Britain £3m-4m (\$5m-6m) to implement a global screening programme that involves regularly checking customer names--and those of third parties involved in their transactions--against United Nations embargo and American sanctions lists for possible terrorist matches. He reckons multinational banks each spend another £2m-3m per year to oversee implementation in their far-flung operations (such institutions commonly have 70 to 100 different transaction

---

<sup>95</sup> *House of Commons Debates*, 067 (23 October 2006) at 4097 (Hon. Judy Sgro); Arar Inquiry Report, *supra* note 6 at 558.

<sup>96</sup> *Supra* note 6

<sup>97</sup> *Supra* note 91

systems). In addition, “tens of millions of pounds” are spent each year in London alone on data storage and retrieval to satisfy a requirement that banks’ client and transaction data be kept for five to seven years. Similar rules exist in America, Singapore and other European countries.<sup>98</sup>

This excerpt suggests that monitoring and reporting of terrorist financing activity is costly, and by implication, has the potential to threaten the economic activity of private businesses.<sup>99</sup> As suggested in the quote above, there will be increases in internal management costs and operational costs on banks themselves as they implement and enforce far-reaching reporting procedures such as those stipulated in the Proceeds of Crime Act. Organizations, especially smaller organizations, may disproportionately bear the reporting burden in terms of costs of monitoring and reporting.

On the other side of the transaction is the customer. If an individual knows that personal information regarding his or her financial transactions will be disclosed or reported, the individual may decide that he or she does not want to “do business” with the bank, despite the fact that the bank is not engaging in terrorist financing at all.<sup>100</sup> There is thus a potential loss of customer base under the legislative scheme. Though the regime is perhaps comprehensive in the reporting procedures it mandates, it may also detract from individuals’ willingness to do business.

The Proceeds of Crime Act thus bears on firms’ efficiency, where efficiency refers to cost-effectiveness. It raises the question of whether the costs of operating the business outweigh the benefits of doing so, and more broadly, whether the costs imposed under the legislation outweigh the benefits to be gained from the scheme. This second issue is an important question that must be raised in any assessment of the regime as a whole. Finally, the legislative regime may be responsible for sending financing of terrorist activities underground to *hawala* and other entities, i.e. away from banks and regulated entities.<sup>101</sup>

---

<sup>98</sup> *Ibid.*

<sup>99</sup> Kevin E. Davis, *supra* note 16 at 185.

<sup>100</sup> *Supra* note 16

<sup>101</sup> See Tom Naylor, *Satanic Purses* (Montreal: McGill-Queen’s University Press, 2006) at 152-166.

*Charities.* Charities may have multifarious purposes, some of which are connected to financing terrorism. The charity as a whole, including the persons for whom the charity functions, can be negatively affected by the acts of some or one of its members. As Davis explains, “funds provided are likely to support both legitimate charitable activities and terrorist activity...subjecting either the organization or its supporters to the harsh sanctions contemplated by counter-terrorism legislation may be a disproportionate response to the threat they pose”.<sup>102</sup> Furthermore, it is not clear that *mens rea* requirements under the Criminal Code could be met in a charity that inadvertently served as a conduit of funds but otherwise serves humanitarian purposes.

Nevertheless, FINTRAC’s 2006 Annual Report states that one third of terrorism financing disclosures involved charities. Thus, perhaps the Bill C-25 amendments, which attempt to create channels of information between FINTRAC and the CRA, are warranted. However, information that can be obtained from the CRA will presumably be limited to registered charities as opposed to entities that purport to operate as non-profits or charities but that are not formally registered as such.

We should remember that organizations engaged in money laundering and/or financing terrorists may not be the type of organizations that view compliance with legal requirements (such as submitting the appropriate taxes and/or documentation with relevant authorities) as their foremost priority. The legislative regime (including the Bill C-25 amendments) may not be effective in combating terrorist financing; they may simply push more and more entities underground in order to achieve their objectives.

## B. Directions

*Assessing Efficacy.* This report does not recommend implementing new laws under the Criminal Code or strengthening the Proceeds of Crime Act. Rather, its focus is on the need to assess the current regime to ensure that its infrastructure functions effectively. In particular, the recommendations relate to assessing the efficacy of the regime; establishing an oversight body for FINTRAC as well as creating an institution that coordinates all anti terrorist financing measures.

---

<sup>102</sup> Davis *supra* note 16 at 184-185.

A full-blown evaluation of anti-terrorist financing laws has not occurred since their implementation a little more than five years ago. As stated in a submission to the Standing Senate Committee on Banking, Trade and Commerce examining Bill C-25, “the questions of proportionality (the extent to which the proposed measures are proportionate and commensurate with the risks at play) and necessity (the extent to which the measures are necessary based on empirical evidence) have not been appropriately addressed.”<sup>103</sup> The time is ripe for such a review and, indeed, the federal government should not implement a new law unless and until the effectiveness of existing laws and institutions are assessed.

As noted above, there are crucial questions that should be examined regarding whether existing laws are effective not only in terms of increased information sharing but in providing to the RCMP and CSIS information that is useful in helping to prevent terrorism. FINTRAC states that it has received numerous reports under the Proceeds of Crime Act. However, it is not clear whether this body is actually catching those individuals who would be involved in terrorist financing. Furthermore, the Criminal Code contains relatively new provisions relating to terrorist financing and it is unclear whether these provisions are effective. Inherent in this assessment would be a statement of the objectives of terrorist financing legislation as a whole and the usefulness of the current means to achieve these objectives. Some questions to be examined are: do the various agencies that have charge over this area of law work co-operatively? If so, is such co-operation effective? If no, should there be an increased emphasis on co-operation?

It is recognized that assessing the impact and effectiveness of a regulatory instrument can be difficult. In the securities regulatory area, for instance, it has taken two decades of examining the low number of convictions in the insider trading area to reveal that either the regulatory regime is ineffective and/or the enforcement of the law has been weak.<sup>104</sup> On the contrary, terrorist financing law is relatively young, which makes evaluation of the efficacy of that law difficult. However, this does not mean that such an evaluation is not warranted, as discussed above. There are means to assess the legal regime. For example, to what extent do reports of suspicious transactions reveal information of actual terrorist financing? How many convictions have there been under the Criminal Code terrorist financing offences? Are the channels that are currently in

---

<sup>103</sup> *Supra* note 16

<sup>104</sup> William J. McNally & Brian F. Smith, “Do Insiders Play by the Rules?” (2003) 29 Can. Pub. Pol’y 125.



place for sharing of information among agencies being utilized? These crucial questions should be examined to assess the current regime. An assessment of the efficacy of existing terrorist financing law is necessary prior to implementing a new law designed to combat the financing of terrorists and terrorist activities.

*Methodology.* Apart from responding to these important questions, it may be useful to conduct either a cost-benefit analysis (CBA) or regulatory impact assessment (RIA) with regards to the current regime. In the securities regulatory field, the U.S. Securities and Exchange Commission, and to a lesser extent the Ontario Securities Commission, routinely incorporate CBA into their rule-making procedure. These CBAs are not usually based in statistical analyses and are qualitative in form.<sup>105</sup> In light of the difficulties in determining whether the regime has been effective in combating the financing of terrorist activity, it is useful to ascertain the benefits of the regime and whether these benefits outweigh its costs. The methodologies for undertaking the CBAs can be complex but they should be explored in the context of assessing the efficacy of the current anti-terrorist financing regime.

Admittedly, while it is possible to be specific in explaining costs and benefits, it is not the case that all costs and benefits are comprehensible or, for that matter, quantifiable. A further weakness of CBA is the variable criteria on which it is based. In light of this problem as well as the difficulty in quantification of costs and benefits, it is worthwhile considering other means of assessing the impact of regulatory initiatives. RIA is a technique that includes CBA but also involves a broader risk-based analysis than CBA entails. CBA does not typically weight risks. That is, it does not consider risk from the standpoint of the relative likelihood of facing specific costs or attaining certain benefits for various relevant stakeholders. For this reason, it may be biased in favour of more regulation since estimated costs of regulation are usually more certain than perceived benefits.

The following steps are often included in an RIA: identifying and quantifying the impact of the legislation; isolating alternatives, which may be non-law based, to address the problem; undertaking risk-based analysis; and, consulting affected parties. RIA also addresses benefits that may not be quantifiable – such as equity and fairness – which are

---

<sup>105</sup> The SEC's use of CBA has been referred to as inadequate and some argue that it has lowered the quality of SEC rulemaking. See Edward Sherwin, "The Cost Benefit Analysis of Financial Regulation" (2005) <http://www.law.harvard.edu/faculty/hjackson/projects.php>.

important, especially from an public interest and protection standpoint. RIA examines the impact that a law has had as well as various alternatives. Who is impacted by the law and what is the range of impact across sectors? RIA is used in the UK which may be a useful jurisdiction to look to in obtaining precedents for such an analysis.

To complete an analysis of costs, benefits and risks (whether in the context of CBA or RIA) it will be necessary for the reviewer to have access to otherwise confidential information. For example, information is generally unavailable regarding the 33 case disclosures made by FINTRAC on terrorism financing. We are unsure whether FINTRAC funneled information relating to these 33 cases to the RCMP or CSIS or both and ultimately what happened with regards to these cases. However, this would be very important information in assessing the efficacy (benefits) of the regime.

In deciding how best to complete an assessment of Canada's terrorist financing regime, the usefulness of Cost Benefit Analysis and Regulatory Impact Assessment should be taken into account.

*Oversight Body.* Canadian law relating to combating terrorist financing is contained in the Criminal Code and in the Proceeds of Crime Act. The Director under the Proceeds of Crime Act is required to report to the Minister "from time to time" on the exercise of the Director's powers and to keep the Minister informed of "any matter that could materially affect public policy of the strategic direction of the Centre."<sup>106</sup> However, no body undertakes an assessment of the efficacy of the existing regime. Indeed, in the absence of such an assessment mechanism, there appears to be an assumption that the regime is effective. Furthermore, Canada has no institution that coordinates the efforts aimed at combating terrorist financing provided under these two pieces of legislation. Terrorist financing also impacts on multiple ministries and agencies within government, making co-ordination and information sharing more difficult. This is unlike the U.S. model where the Office of Terrorism and Financial Intelligence is a body that consolidates the policy, enforcement, regulatory and international functions of the U.S. Treasury relating to terrorist financing.

---

<sup>106</sup> *Proceeds of Crime Act*, *supra* note 5, sections 52(1)-(2).

With regards to Canadian federal initiatives to combat terrorist financing, there is certainly the potential for coordination (particularly in the area of information sharing) among Canadian institutions such as FINTRAC, the RCMP, CSIS etc. For efficiency purposes, it stands to reason that information sharing and other forms of cooperation should occur, and, perhaps should be mandated. Legal parameters that govern information sharing among these agencies may need to be established to ensure that the information sharing occurs “in a reliable and responsible fashion”.<sup>107</sup> An oversight or umbrella organization that coordinates the activities of these various institutions may also be warranted.

Some may look to FINTRAC as capable of coordinating activities among the various institutions at work in combating terrorist financing. However, FINTRAC’s mandate is limited to the Proceeds of Crime Act and terrorist financing law clearly extends beyond this one statute. Furthermore, in light of the privacy and efficacy issues raised in this report, it stands to reason that there should be a separate body that oversees FINTRAC’s operations. This independent reviewer would be responsible not only for evaluating the activities of FINTRAC but also for coordinating all of the laws relating to the financing of terrorism and perhaps assessing the effectiveness of the current regime. As the Auditor General has stated, “the government should assess the level of review and reporting requirements to Parliament for security and intelligence agencies to ensure that agencies exercising intrusive powers are subject to levels of external review and disclosure proportionate to the level of intrusion.”<sup>108</sup>

The question remains as to who the independent reviewer should be. There are a number of options here beginning with the Auditor General, some sort of Ministerial oversight, Parliamentary Committee, or SIRC. Notably, the Arar Inquiry Report recommended that SIRC’s role should be expanded to review national security activities of FINTRAC.<sup>109</sup> However, SIRC deals mainly with issues of propriety, its mandate being to “review generally the performance of the Service [CSIS] of its duties and functions”.<sup>110</sup> In light of the argument here in favour of an oversight body that can deal with issues of efficacy, it appears that SIRC may not be the appropriate body to perform this oversight role. Further study is warranted on whether existing institutions are able to take on this oversight function and how the oversight will be performed.

---

<sup>107</sup> *Supra* note 5

<sup>108</sup> *Supra* note 7

<sup>109</sup> *Arar Events Report*, *supra* note 7 at 573.

<sup>110</sup> *Supra* note 7



Study should be accorded as to whether an oversight body is warranted to consolidate the policy, enforcement and regulatory processes currently in place to combat terrorist financing, and, if so, whether existing institutions are able to take on this oversight function and how the oversight will be performed.

*Overseeing FINTRAC.* FINTRAC receives information from various sources (CBSA, CSIS, RCMP) but is permitted to disclose only certain designated information. The structure of FINTRAC, and these rules in particular, are meant to balance competing objectives. The result however is a body that lacks transparency, as the recent Arar Inquiry Report pointed out.<sup>111</sup> For a number of reasons, it makes sense to have a body that oversees FINTRAC and that examines a variety of questions on a periodic basis. First, is FINTRAC performing its functions effectively (per the above discussion)? Second, to what extent are privacy rights sacrificed? Third, is FINTRAC complying with the statute that provides its mandate and is it administering the statute appropriately? Finally, should more information sharing occur?

At present, FINTRAC is subject to certain oversight procedures in the Proceeds of Crime Act. Specifically, it must submit an annual report on its operations to the Minister and the Minister will table a copy of the report in Parliament.<sup>112</sup> In addition, the administration and operation of the Act will be subject to a five-year review by a committee of Parliament under Bill C-25.<sup>113</sup> All receipts and expenditures of FINTRAC are subject to examination and audit.<sup>114</sup> Although FINTRAC can be the subject of suits and legal proceedings,<sup>115</sup> no action lies against any of the employees of the Centre if they have acted in good faith in discharging their duties.<sup>116</sup>

While the Act will be reviewed every five years by a Committee of Parliament, there is no body that reviews FINTRAC's operations and the efficacy of those operations. There is some merit, therefore, in having a review committee with the powers and authority to conduct random reviews of FINTRAC's files, operations and compliance with its governing statutes and other law. This is a recommendation made by the Senate

---

<sup>111</sup> *Arar Events Report*, *supra* note 7 at 567.

<sup>112</sup> *Supra* note 7

<sup>113</sup> *Supra* note 5

<sup>114</sup> *Proceeds of Crime Act*, *supra* note 5, section 70(1).

<sup>115</sup> *Supra* note 5

<sup>116</sup> *Ibid.*, section 69.



Committee on Banking Trade and Finance which stated that FINTRAC should be subject to an annual review, and the reviewing body should be SIRC.<sup>117</sup> While this report makes no suggestion regarding the precise body that takes on the oversight function, it does point to the necessity of such an overseer.

Consideration should be given to the issue of whether an oversight body that monitors the activities of FINTRAC with respect to its efficacy as well as the propriety of its operations on a periodic basis is warranted.

Admittedly, a danger exists in focusing only on FINTRAC in the proposed review and monitoring system. Presumably, such a review would focus only on the flow of information into and out of FINTRAC but not necessarily on actions taken with respect to that information once it is handed over to other bodies such as the RCMP, CSIS or foreign agencies. Thus, in keeping with the discussion throughout this section, the oversight body should be charged not only with monitoring FINTRAC, but also with overseeing all entities that play a role in anti-terrorist financing activities including those of CSIS and the RCMP.

## 5. CONCLUSION

The Canadian regime that governs the financing of terrorism is relatively new – it has been in existence for less than a decade. It is difficult to know at this time whether the regime has been and is effective in combating the financing of terrorism. However, this is not to say that the regime is ineffective. Rather, before any new law is implemented, an assessment of the efficacy and efficiency of the current regime is required. This assessment would be a first step towards understanding whether (and where) additional laws are necessary. This is a pragmatic approach. Our expectations about what law can achieve should be reasonable and well informed. That is, we should not advocate a specific set of legal reforms in the absence of evidence that this particular reform (as opposed to other available alternatives) is warranted. This is because regulation is costly in the sense that it imposes burdens on the regulated. Those burdens may indeed be justified but they must be proven to be so. Otherwise, the regulation is nothing more than an experiment, and usually a costly one.

---

<sup>117</sup> *Senate Committee Report, supra* note 91 at 22.

**Anita Indira Anand**, BA (Hons) (Queen's) 1989, BA (Hons in Jurisprudence) (Oxon) 1991, LLB (Dalhousie) 1992, LLM (Toronto) 1996, joined the University of Toronto Faculty of Law from Queen's University where she was an Associate Professor (2003-2006) and Assistant Professor (1999-2003). She currently serves as Associate Dean (JD Program) at the Faculty of Law at Toronto. In 2006, she was a Canada-U.S. Fulbright Scholar and Visiting Olin Scholar in Law and Economics at Yale Law School. During the Fall 2005, she was a Visiting Lecturer in Law at Yale Law School where she taught comparative corporate governance. She is the recipient of research grants from the Social Sciences and Humanities Research Council of Canada (two awards) and the Foundation for Legal Research (three awards) as well as the Canadian Association of Law Teachers' Scholarly Paper Award (2003). In Fall 2004, she received the Queen's Law Students' Society Award for Excellence in Teaching and in Fall 2006, she and co-authors Frank Milne and Lynnette Purda were awarded the Best Paper in Managerial Finance by the International Journal of Managerial Finance for their empirical research relating to corporate governance. She has published articles in the University of Toronto Law Journal, the McGill Law Journal, the Delaware Journal of Corporate Law, the Stanford Journal of Law, Business and Finance, the NYU Journal of Law and Business and has co-authored the book *Securities Regulation: Cases, Notes and Materials* with Mary Condon and Janis Sarra. Professor Anand has conducted research for the Five Year Review Committee, the Wise Person's Committee, and the Task Force to Modernize Securities Legislation in Canada. She is the Editor of Canadian Law Abstracts, published by the Legal Scholarship Network and the Vice President (President Elect) of the Canadian Law and Economics Association. Her main research and teaching areas are corporate law, securities regulation, and bankruptcy and insolvency law.

**Terrorist Financing and the Charitable Sector:**

**Law and Policy in the United Kingdom, the United States,  
and Australia**

**Research paper prepared for the Commission of Inquiry  
into the Investigation of the Bombing of Air India Flight 182,  
Government of Canada**

**Mark Sidel**

**Professor of Law and International Affairs  
and Faculty Scholar, University of Iowa**

## **Introduction: Issues in Terrorist Finance and the Role of Charities in Comparative Perspective**

This research paper addresses measures by government to prevent charities from playing a role in terrorist finance while maintaining the autonomy and vibrancy of the charitable sector.<sup>1</sup>

Terrorists and terrorist organizations may be financed through many methods and mechanisms. This paper addresses one such mechanism – the use of charitable organizations to funnel funds to terror-related individuals and organizations. Charities may be aware or unaware of their use for terrorist financing, and where appropriate this paper addresses both possibilities. The paper begins from the premise that democratic societies and their charitable sectors generally seek to prevent charities from being used as conduits to terrorism, and that this policy intention provides some commonality of purpose between government and the charitable sector.

There are significant differences in the way that the nexus between charitable organizations, terrorism, and terrorist finance is regulated in the U.K., the U.S., and Australia. The British approach has relied significantly on charity regulators as statutory-based core partners in the battle against terrorism, often as “first responders” in situations where charities are allegedly tied to terrorism or terrorist finance. The American approach to shutting off terrorist finance from nonprofits largely sidesteps charity regulators in favor of direct action by prosecutors, a function of both prosecution- and homeland security-led counter-terrorism measures in the United States and the bifurcated nature of nonprofit regulation under the American federal structure. Australia may be somewhere in between, relying primarily on prosecution and security-led approaches, but also perhaps without sufficient data to characterize actual practice.

The paper begins from the important premise that measures used to monitor, investigate, restrict, prosecute or otherwise affect charities in the goal of restricting terrorist financing should also seek to maintain the autonomy and vibrancy that characterizes the charitable sector in democratic societies, and that serious efforts must be made to balance society’s interests in freedom from terrorism with society’s interests in a vibrant, autonomous and powerful charitable sector.

---

<sup>1</sup> Opinions expressed are those of the author and do not necessarily represent those of the Commission or the Commissioner.



These are not the “state’s” interests distinguished from the “charitable sector’s” interests; our interests in combating terrorism and in preserving and enhancing the vital role of the charitable sector are interests that states and charitable sectors share, as do other forces in society.

What measures are the United Kingdom, the United States and Australia and the United States using to prevent the use of charities in terrorist financing? Have those means been effective? How do the various mechanisms used affect or restrict the autonomy and vibrancy of the charitable sector and its work? Are countries able to maintain an effective balance between the crucial societal interests in security and in charitable autonomy and vibrancy?

Another researcher, Professor David Duff of the University of Toronto Faculty of Law, is addressing these issues specifically for Canada. These papers are thus complementary, though they do not necessarily express a common viewpoint.

As I have indicated in other work,<sup>2</sup> conflict between governments and the charitable sector (sometimes called the nonprofit, not-for-profit, or “third” sector) is growing in a number of countries. A significant reason for that growing conflict and mistrust is the perception on the part of a number of governments that the charitable sector is a link to terrorism, through financing, ideology, and facilitating meetings and organization.

More broadly, a number of governments do not now appear to regard the charitable sector as a source of human security. Rather, they seem to regard the third sector as a source of insecurity, not as civil society but as encouraging uncivil society, not as strengthening peace and human security, but as either a willing conduit for, or an ineffective, porous and ambivalent barrier against insecurity in the form of terrorism and violence.

There has always been mistrust of the voluntary sector by governments in many nations around the world. This mistrust is expressed by governments in tightened regulation, stricter governance and financial

---

<sup>2</sup> Mark Sidel, *The Third Sector, Human Security, and Anti-Terrorism in Comparative Perspective* (Keynote address delivered to the Seventh International Conference of the International Society for Third Sector Research (ISTR)), Bangkok, July 2006); Mark Sidel, *The Third Sector, Human Security, and Anti-Terrorism: The United States and Beyond*, 17 *Voluntas: International Journal of Voluntary and Not-for-Profit Organizations* 199-210 (2006).

requirements, restrictions on foreign funding, limitations on endowment growth and investments, barriers to advocacy, and a host of other legal and policy requirements. But for a number of governments, the current suspicion of the charitable sector goes beyond traditional mistrust or skepticism and reflects a vision of the charitable sector as a source of insecurity and incivility that has fueled the reemergence of terrorism, particularly in the wake of the 2001 and subsequent attacks in Bali, London, Madrid, and elsewhere. The charitable sector is now under suspicion and investigation for the role – real or alleged – that some charitable organizations may have played in ties to terrorism. And even where governments do not make the explicit ties between the charitable sector and terrorism, the sector is generally regarded as easily used by terrorism, an ineffective and porous source of finances, organization, communications, and the transfer of goods and services for terrorist purposes.

The ripples of this pressure on the charitable sector travel far indeed. The perception that civil society is indeed uncivil and a source of insecurity contributes to an environment of enhanced regulation of the voluntary sector, strengthened state oversight of voluntary sector activities, and declining confidence in the sector's ability to contribute to the resolution of social problems and the advancement of human security. Governments that believe that the third sector is a conduit for terrorism and a source of human insecurity may respond with heightened regulation of the charitable sector, including new or enhanced financial, governance, reporting or other restrictions. Sometimes these policies may be relatively informal, more along the lines of what Professor Jude Howell has called the "intangible creation of climates of opinion or shifting attitudes" toward the voluntary sector.<sup>3</sup>

Although this research paper specifically addresses government measures to prevent the use of charities as conduits for terrorist financing in Australia, the United Kingdom, and the United States, these are issues in a wide range of countries, including Australia, Cambodia, Canada, the countries of Central Asia, China, India, the Netherlands, Pakistan, the United Kingdom, Pakistan, Zimbabwe, and elsewhere throughout Asia, Africa, and Latin America.

---

<sup>3</sup> Comments by Professor Howell at the Program on Terrorism and Development, London School of Economics, 17 October 1995 ([www.lse.ac.uk/collections/LSEPublicLecturesAndEvents/pdf/20051017-TerrorismAndDevelopment.pdf](http://www.lse.ac.uk/collections/LSEPublicLecturesAndEvents/pdf/20051017-TerrorismAndDevelopment.pdf)).

Government responses may take many specific forms, including prevention of terrorism laws and regulations in India and elsewhere in South Asia that directly affect the nonprofit sector (India and elsewhere in South Asia); enhanced restrictions on gatherings and associational activities (China); limitations on funding and new certification requirements for funders and nonprofits alike (the United States); inclusion of charities in new anti-terrorism legislation and enhanced investigations (the United Kingdom); and a host of other measures.<sup>4</sup>

It is also important to note that the idea that the charitable sector is a source of insecurity, even a conduit of terrorism, may not be the primary factor in state attempts to monitor or tighten control over the sector. Other factors can play a major role in such policies. They include the rapidly growing role of diasporas in social development, and the attention that brings from the state, concerns about accountability and transparency in the voluntary sector, the growing role of political and religious giving, and a number of other factors.

The state policies may, depending on the country context, contribute to declining funding for the sector, a declining ability for the charitable sector to obtain support for innovative programs, and an atmosphere of investigation and suspicion that may envelop the sector. State policies may contribute to a shifting of aid priorities including preferences for anti-terrorism programs in foreign aid. And such government policies may contribute to timidity within the charitable sector that may lead to refusal

---

<sup>4</sup> The growing academic and practice literature on government-charitable sector relations and anti-terrorism includes Richard Moyers, A Shocking Silence on Muslim Charities, *Chronicle of Philanthropy*, 17 October 2002; Barnett Baron, Deterring Donors: Anti-Terrorist Financing Rules and American Philanthropy, *International Journal of Not-for-Profit Law* 6(2): 1-12 (2004); InterAction, *Handbook on Counter-Terrorism Measures: What U.S. Nonprofits and Grantmakers Need to Know* (2004); Kumi Naidoo, Coming Clean: Civil Society Organisations at a Time of Global Uncertainty, *International Journal of Not-for-Profit Law* 6(3): 1-3 (2004); Alan Fowler, *Aid Architecture: Reflections on NGDO Futures and the Emergence of Counter-Terrorism* (INTRAC Occasional Papers Series No. 45, Oxford, 2005); Teresa Odendahl, *Foundations and their Role in Anti-terrorism Enforcement: Findings from a Recent Study and Implications for the Future*, Georgetown University, June 2005; Blake Bromley, *The Post 9/11 Paradigm of International Philanthropy* (Paper presented to the International Society for Third Sector Research Seventh International Conference, Bangkok (July 2006)); Terrence Carter, *The Impact of Anti-Terrorism Legislation on Charities: The Shadow of the Law* (Carters, Toronto, 2006); Civicus, *Impact of Counterterrorism Measures on Civil Society* (Civicus, Southdale (South Africa), 2006); Jude Howell, *The Global War on Terror, Development and Civil Society*, *Journal of International Development* 18: 121-135 (2006); Mark Sidel, *More Secure, Less Free? Antiterrorism Policy and Civil Liberties after September 11* (University of Michigan Press, 2004, revised ed. 2006); C.R.M. Versteegh, *Terrorism and the Vulnerability of Charitable Organisations*, Paper presented to the International Society for Third Sector Research Seventh International Conference, Bangkok (July 2006).

to engage in important and innovative but also perhaps controversial work at a time when charities are under pressure in a number of countries and intense pressure in a few. Finally, these conflicts and circumstances demand that the charitable sector do more, and do more effectively, to regulate itself.

A related problem is the limits of terrorist finance law in preventing terrorism, particularly in the context of charities. Can laws against terrorist finance and penalties on charities significantly assist in stopping terrorism when terrorists and their supporters may have multiple means to channel funds? When at least some forms of terrorism can be financed at a relatively low cost? The effectiveness of the law in stopping terrorism is necessarily part of an assessment of charities regulation and terrorist finance that takes into account proportionality and balancing.

A third related theme is the role of state registration, certification or approval of a charity's formation and continued existence. Terrorist victims may believe that government acquiescence in the establishment and operations of a charitable organization that is accused of political or ideological support for causes that are also supported by terrorism reflects state ignorance, indifference or even support for such causes. In a pluralist democracy, government acquiescence in the formation and continued operation of a voluntary organization – as long as it does not violate terrorist finance or other laws – does not constitute endorsement of the charity's political view. But some citizens do believe that charities regulation should be used to proscribe or limit the activities of voluntary organizations that hold extremist views, even if they do not violate the law.

## **II. United Kingdom**

### **The Framework of Anti-Terrorist Law and Policy**

British law and policy with respect to charities and terrorist finance has, in one key respect, been consistent with developments in the United States and other countries. British law allows proscription of terrorist organizations, bans support for such proscribed organizations, helping such organizations arrange or manage meetings to further their activities. British law also more broadly bans fundraising and making various kinds



of funding arrangements for “purposes of terrorism”. It also prohibits retention or control of “terrorist property.”<sup>5</sup>

But state policy has gradually expanded to the point that new legislation adopted in 2006 (the Terrorist Act 2006) criminalizes not only direct support for terrorist organizations and activities, but “encouragement,” “glorifying,” and other activities more closely related to freedom of speech and freedom of association. This seemingly inexorable expansion of mandates for the charitable sector puts particular pressure on charitable organizations affiliated with certain religious and ethnic groups.

The primary anti-terrorism legislation affecting charities in the U.K. is the Terrorism Act 2000, which entered into force in February 2001. The Terrorism Act 2000 gives the Secretary of State authority to proscribe an organization if the Secretary “believes that it is concerned in terrorism.” “Concerned in terrorism” is defined broadly as “commits or participates in acts of terrorism, prepares for terrorism, promotes or encourages terrorism, or is otherwise concerned in terrorism either in the UK or abroad.” An organisation may be “any association or combination of persons.” Proscribed organization membership is illegal, as well as assisting, fundraising, providing funds to such an organisation or any member, or to belong to, support, or display support for a proscribed organization. All property of a proscribed organization may be seized by the government. Organizations are allowed to apply for de-proscription, and an appeals process is provided for organizations denied de-proscription.<sup>6</sup>

The Terrorism Act 2000 also criminalizes membership in a proscribed organization (sec. 11); it also criminalizes various forms of support for proscribed organizations, including the offenses of “invites support” (not limited to financial support for a proscribed organization (sec. 12(1)); “arranges, manages or assists” in arranging meetings for a proscribed organization (sec. 12(2)); wearing the uniform of a proscribed organization

<sup>5</sup> Legal Opinion by Edward Fitzgerald Q.C. and Caoilfhionn Gallagher, Doughty Street Chambers, London, in National Council of Voluntary Organisations (NCVO), Security and Civil Society (January 2007) ([www.ncvo-vol.org.uk](http://www.ncvo-vol.org.uk)).

<sup>6</sup> Terrorism Act 2000, Part II, Sec. 3. See Charity Commission, Operational Guidance: Charities and Terrorism, OG96-28 (January 2003) ([www.charity-commission.gov.uk/tcc/terrorism.asp](http://www.charity-commission.gov.uk/tcc/terrorism.asp)). A list of proscribed organizations is provided at the end of OG96-28 Operational Guidance. See also Home Secretary Moves to Ban 15 Terror Groups, Home Office, Press Office, 10 October 2005 (press. [homeoffice.gov.uk/press-releases](http://homeoffice.gov.uk/press-releases)) (containing a full banning order and additional information).

(sec. 13). More broadly the Terrorism Act 2000 also criminalizes fund-raising for “purposes of terrorism” (sec. 15); use of money or other property for purposes of terrorism (sec. 16); undertakes other funding arrangements for purposes of terrorism (sec. 17); or engages in broadly defined money laundering of terrorist property (sec. 18).<sup>7</sup>

In addition, the Charity Commission has the statutory power under the Regulation of Investigatory Powers Act 2000 and the Serious Organised Crime and Police Act 2005 to “send ‘Covert Human Intelligences Sources’ ... i.e. spies or undercover agents, to work in charities that are under suspicion.”<sup>8</sup>

### **The Role of the Charity Commission: Keeping Charity Regulators Central in Terrorist Finance Enforcement**

A difference in the British context is that while the American approach to shutting off terrorist finance from nonprofits largely sidesteps charity regulators in favor of direct action by prosecutors, the British approach has, at least in part, relied on charity regulators as partners and, often but not always, “first responders” in the antiterrorist enterprise.<sup>9</sup> The Charity Commission is the central regulator and registrar for charities in England and Wales. It has been key to these efforts and has played a core role in investigating, resolving and where necessary collaborating in prosecuting ties between charities, terrorism, and terrorist finance. Its central role has been reaffirmed under the new Charities Act 2006.<sup>10</sup>

Of course, that approach is not the only possible means of attack on this issue. Charities have been used to funnel funds to external terrorist groups in Britain, as in the United States and other countries, and the government moved quickly after September 11 to enforce the U.N. resolutions that called for freezing funds held by Al Qaeda, the Taliban and other terrorist groups. So clearly prosecution has an important role to play as well and this is clearly recognized by the Charity Commission.

---

<sup>7</sup> Terrorism Act 2000, Part III, Secs. 14-19.

<sup>8</sup> Legal Opinion by Edward Fitzgerald Q.C. and Caoilfhionn Gallagher, Doughty Street Chambers, London, in NCVO, *Security and Civil Society* (January 2007), at [www.ncvo-vol.org.uk](http://www.ncvo-vol.org.uk). Whether government bodies agree that they have this statutory power has not yet been confirmed.

<sup>9</sup> See also the author's discussion of British approaches to antiterrorism and the nonprofit sector in Sidel, *More Secure, Less Free?* (University of Michigan Press, 2004, revised ed. 2006).

<sup>10</sup> For detailed information on the role and functions of the Charity Commission, see <http://www.charity-commission.gov.uk/tcc/ccabout.asp>, and, for summary information on the Charities Act 2006, <http://www.charity-commission.gov.uk/spr/ca2006prov.asp>.

Charity regulators in the United States – for example, well-informed specialists in the U.S. Treasury Department's Exempt Organizations Division – appear somewhat marginalized in the enforcement of laws against terrorist financing by charities in the U.S. because of the structure of nonprofit regulation in the United States, historical limitations on their roles, and the prosecution-centered nature of antiterrorist law and policy in the U.S. But their counterparts, charity regulators in the U.K., appear to play a more central role than federal charity regulators in the United States. That different structure has been to Britain's advantage in working out a response to the uses of charities by terrorist organizations in the post-September 2001 era that has helped keep charity regulators directly involved in anti-terrorist policy and activities.

In Great Britain, the key charity regulator is the Charity Commission, which has been near the forefront of charity-related terrorism financing investigations since before September 11. The Charity Commission certainly had jurisdiction over investigations of charitable links to terrorism in England and Wales before the September 2001 attacks. For example, the Commission had already investigated the North London Central Mosque Trust (Finsbury Park Mosque), which Sheikh Abu Hamza al-Masri (Abu Hamza) had taken over in the late 1990s. In that earlier proceeding, after Commission investigation, the original mosque trustees had reached an agreement with Abu Hamza in which the trustees would resume "full control of the Mosque and other property" in exchange for Abu Hamza being permitted to give half of the Friday sermons at the Mosque (later three out of four sermons).<sup>11</sup>

But Abu Hamza's control of the Mosque persisted, and the more moderate trustees were forced to the sidelines until the Charity Commission intervened again. This was done after 2001 and effectively removed Abu Hamza and returned the Mosque to proper control. This approach was effective because of the Charity Commission's wide investigatory and enforcement powers and its detailed understanding of developments in the charitable sector including the North London Mosque. In addition, the Commission had an array of means at its disposal to resolve charitable failures to abide by the law – ranging from technical assistance and advice to agreements to change practices to, where needed, orders removing trustees, freezing funds, or closing organizations.

---

<sup>11</sup> Charity Commission, Inquiry Report: North London Central Mosque Trust (2003) | [www.charitycommission.gov.uk/news/mosqueinq.asp](http://www.charitycommission.gov.uk/news/mosqueinq.asp)).



The Charity Commission's role in this area accelerated after 2001, initially with an investigation of the U.K.-registered International Islamic Relief Organization after a *Times of London* report that "the charity was under CIA scrutiny in connection with the possible transfer of funds which may have been used to support the terrorist attacks in the United States." That inquiry was closed a month later after the Commission determined that the organization had ceased to operate in the U.K. and removed it from the register of charities.<sup>12</sup>

A number of other inquiries have taken place since the September 11 attacks, as the Commission reaffirmed that "any kind of terrorist connection is obviously completely unacceptable [and] investigating possible links with terrorism is an obvious top priority for the charity commission." But in doing so the Commission also sought to assuage fears of a witch-hunt: "The good news is that, in both absolute and relative terms, the number of charities potentially involved are small. Neither the charity commission, nor other regulatory and enforcement organizations have evidence to suggest that the 185,000 charities in England and Wales are widely subject to terrorist infiltration."<sup>13</sup>

The Charity Commission's role in investigating charitable links to terrorism has continued and expanded in recent years. In May 2002, the Commission reported that it had "evaluated concerns" about ten charities since the September 11 attacks, "opened formal inquiries" into five, closed two, and frozen the assets of one group.<sup>14</sup> "Vigilance is everything," the Commission warned: "Any links between charities and terrorist activity are totally unacceptable. Links ... might include fundraising or provision of facilities, but also include formal or informal links to organizations 'proscribed' under the Terrorist Act 2000, and any subsequent secondary legislation."

But the Commission also emphasized that its relationship to the charitable sector was useful in the antiterror battle, and that charities would not be left out of the process. "[T]he Charity Commission is committed to working with the sector it regulates – to ensure that terror groups are never allowed to gain a foothold within England and Wales; 185,000 registered charities." And an important responsibility would

---

<sup>12</sup> Debra Morris, Charities and Terrorism: The Charity Commission Response, *International Journal of Not-for-Profit Law* (September 2002) ([www.icnl.org](http://www.icnl.org)).

<sup>13</sup> John Stoker, Weeding Out the Infiltrators, *The Guardian* (U.K.), 28 February 2002.

<sup>14</sup> Charity Commission, Charity Commission Policy on Charities and Their Alleged Links to Terrorism (May 2002) ([www.charity-commission.gov.uk/tcc/terrorism.asp](http://www.charity-commission.gov.uk/tcc/terrorism.asp)).



continue to fall to trustees to “take immediate steps to disassociate” any charity from links to terrorist activity and to “be vigilant to ensure that a charity’s premises, assets, volunteers or other goods cannot be used for activities that may, or appear to, support or condone terrorist activities...” Accountability and transparency – not only prosecution – were crucial to that process,<sup>15</sup> and particularly crucial was the existence and clear role of the Charity Commission.

As investigations continued, more guidance was clearly needed for charitable organizations. The Commission issued “operational guidance” on “charities and terrorism” in January 2003 that reaffirmed the Commission’s central role in investigating alleged charitable links to terrorism and enforcing law and policy with respect to the sector. The 2003 operational guidance also reconfirmed the close relationship between the Commission – through its Intelligence and Special Projects Team (ISPT) – and other law enforcement, security and intelligence organizations.<sup>16</sup> Later that spring, the Commission issued guidelines for charities working abroad that focused on the risk that charitable funds would reach terrorist organizations and did not appear to impose as many new burdens on charities as their American counterpart guidelines.<sup>17</sup>

Throughout this work a recurring theme was the notion that the Commission should remain at the forefront of work against the use of charities in terrorist financing, seeking to retain cooperation with the voluntary sector while combating terrorism, rather than ceding that work to security and police organizations. That fit well with the Commission’s traditional role. As the Commission’s annual report for 2002 and 2003 put it, perhaps in a broader context, the goal was “maintaining our independence and working with others.”<sup>18</sup>

### **North London Central Mosque (Finsbury Park Mosque) (2001-2003)**

Investigations have continued. The most prominent has been the Commission’s long engagement with the problems of the North London

<sup>15</sup> Id.

<sup>16</sup> Charity Commission, Operational Guidance: Charities and Terrorism, OG96-28 (January 2003) ([www.charity-commission.gov.uk/tcc/terrorism.asp](http://www.charity-commission.gov.uk/tcc/terrorism.asp)).

<sup>17</sup> Charity Commission, Charities Working Internationally (2003) ([www.charity-commission.gov.uk/tcc/terrorism.asp](http://www.charity-commission.gov.uk/tcc/terrorism.asp)).

<sup>18</sup> Charity Commission Annual Report 2002-2003.

Central Mosque (Finsbury Park Mosque) and its radical, anti-American leader until 2004, Sheikh Abu Hamza al-Masri. Abu Hamza and his followers had taken over the mosque from more moderate trustees and were using it for extremist religious and political purposes. After the September 11 attacks, the Commission renewed earlier investigations of the mosque and Abu Hamza's role, upon receiving tapes of sermons that were "of such an extreme and political nature as to conflict with the charitable status of the Mosque" and an investigatory report of a "highly inflammatory and political conference" at the mosque on the first anniversary of the World Trade Center and Pentagon attacks.

In cooperation with police and security agencies and with the support of the mosque's original trustees, in a 2003 decision the Commission suspended Abu Hamza from his position within the mosque, froze mosque accounts controlled by Abu Hamza and in February 2003 removed him from all positions in the mosque. At the same time the London police secured the mosque and handed it back to the original trustees.<sup>19</sup> In undertaking this complex task the Charity Commission was aided by the wide array of powers at its disposal. These powers included freezing funds, appointing substitute trustees and auditors, ordering specific activities or organizations shuttered for periods of time, and other measures. The Commission was also assisted by its detailed knowledge of the Mosque gained through a number of years of charity enforcement.

In May 2004, U.S. Attorney General Ashcroft unsealed an eleven count indictment charging Abu Hamza with conspiracy to provide material support to terrorists, assistance to a 1998 bombing in Yemen and other offenses. The British authorities arrested Abu Hamza at the request of the U.S. government and prepared to extradite him to the United States. In 2006 Abu Hamza was sentenced to seven years imprisonment in the U.K. for counseling murder and racial hatred.<sup>20</sup>

## **Society for the Revival of Islamic Heritage (2002)**

The Charity Commission conducted a number of other investigations into alleged charitable links with terrorism, not all with similarly dramatic

<sup>19</sup> Charity Commission, Inquiry Report: North London Central Mosque Trust (2003) ([www.charity-commission.gov.uk/news/mosqueinq.asp](http://www.charity-commission.gov.uk/news/mosqueinq.asp)); British Arrest Radical Cleric U.S. Seeks, *New York Times*, 28 May 2004. See also extensive coverage of the Abu Hamza case in British newspapers, especially *The Times* (London) and *The Guardian*, in May and June 2004. For a sense of the different atmosphere at the mosque in 2005, see At Mosque That Recruited Radicals, New Imam Calls for Help in Catching Bombers, *New York Times*, 9 July 2005.

<sup>20</sup> Abu Hamza Convicted, *The Guardian* (London), 8 February 2006. Such a prosecution might be more difficult in the United States because of speech protections.

conclusions. A 2002 inquiry into the Society for the Revival of Islamic Heritage was prompted by notice that the U.S. Treasury Department had issued a blocking order against a group with a similar name that had offices in Pakistan and Afghanistan, and that the U.S. government believed that that the group “may have financed and facilitated the activities of terrorists ... through Usama Bin Laden.” After investigating possible ties between the organization registered in London and the group proscribed by the United States, the Commission found no evidence linking the U.K. charity with the U.S.-banned group, and closed its inquiry.<sup>21</sup>

### **Minhaj-UI-Quran UK and Idara Minhaj-UI-Quran UK (2002)**

Another inquiry was launched in 2002 after allegations that the London-based Minhaj-UI-Quran UK and Idara Minhaj-UI-Quran UK was “supporting political activities in Pakistan.” There were also allegations that the records kept at the Charity were poor and that its financial controls were weak. After investigation, the Commission cleared the charity of the political support allegations that had been made against it. The Commission did, however, order the group to strengthen accounting controls, and reached an agreement with the trustees on new controls.<sup>22</sup> This case demonstrates the Commission’s ability to investigate both a charity’s internal functions, as well as whether it has improper ties.

### **Divergence from the United States: The Interpal Case (2003)**

In response to a U.S. allegation that funds from the Palestinians Relief and Development Fund (Interpal) were going to Hamas, the Commission contacted Interpal in April 2003 to determine whether Interpal funds had gone for “political or violent militant activities” of Hamas in Palestine. This followed a 1996 investigation of Interpal that had found “no evidence of inappropriate activity, and the information available indicated that Interpal was a well-run organization.”

<sup>21</sup> Charity Commission, Trustees Have No Link with Terrorism (Press Release PR02/02), 5 November 2002 ([www.gnn.gov.uk/environment\\_detail.asp?ReleaseID=31336&NewsAreaID=2&NavigatedFromDepartment=True](http://www.gnn.gov.uk/environment_detail.asp?ReleaseID=31336&NewsAreaID=2&NavigatedFromDepartment=True)). Unfortunately we do not know with certainty whether the Commission found no evidence, or no evidence that rose to a useable or probative level. The Commission is required to maintain confidentiality of sensitive security information.

<sup>22</sup> Charity Commission, Inquiry Report: Minhaj UI-Quran UK, 2002 ([www.charity-commission.gov.uk/inquiryreports/minhaj.asp](http://www.charity-commission.gov.uk/inquiryreports/minhaj.asp)); and Inquiry Report: Idara Minhaj-UI-Quran UK, 2002 ([www.charity-commission.gov.uk/inquiryreports/idara.asp](http://www.charity-commission.gov.uk/inquiryreports/idara.asp)).



The initial 2003 investigation by the Commission found that Interpal had “improved its procedures and record keeping since the Commission’s previous Inquiry, although these procedures could be further enhanced by introducing a greater degree of independent verification of the work done by Interpal’s partners in the region on its behalf.” The Inquiry also turned up evidence that Interpal had received funds from an organization proscribed under U.N. sanctions in May of 2003, the Al-Aqsa Foundation, though “the funds received were in respect of humanitarian work already carried out by Interpal and then invoiced” to Al-Aqsa.

While the Commission’s Inquiry was underway, the U.S. government formally named Interpal as a “specially designated global terrorist” organization and proscribed its activities in the United States “for allegedly supporting Hamas’ political or violent militant activities.” The Commission immediately opened a formal Inquiry under section 8 of the Charities Act 1993 and froze Interpal’s accounts “as a temporary and protective measure.” The Commission also requested “evidence to support the allegations made against Interpal” from the United States, but, according to an understandably limited report from the Commission, the U.S. was “unable to provide evidence to support allegations made against Interpal within the agreed timescale.”<sup>23</sup>

In late September, the Commission decided “in the absence of any clear evidence showing Interpal had links to Hamas’ political or violent militant activities” that Interpal’s accounts would be unfrozen and the Commission’s Inquiry closed.

The Interpal Inquiry also enabled the Commission to reassert that it will “deal with any allegation of potential links between a charity and terrorist activity as an immediate priority ... liais[ing] closely with relevant intelligence, security and law enforcement agencies to facilitate a thorough investigation.” The Commission also reemphasized that “as an independent statutory regulator the Commission will make its own decisions on the law and facts of the case.”<sup>24</sup>

The British bank NatWest has also been sued by people or their relatives wounded in suicide bombings in Israel, in cases where Hamas has claimed that it carried out the bombings, based on claims that NatWest sent

<sup>23</sup> From the Commission reporting on this matter is it not clear if the issue was that there was no evidence or that the United States was unwilling to disclose the intelligence that it might have had.

<sup>24</sup> Charity Commission, Inquiry Report: Palestinians Relief and Development Fund, 2003 ([www.charity-commission.gov.uk/investigations/inquiryreports/interpal.asp](http://www.charity-commission.gov.uk/investigations/inquiryreports/interpal.asp)).



funds through accounts held by Interpal to Hamas. NatWest called the suit “without merit,” contested it in New York, and said that the Charity Commission had “found no evidence of wrongdoing” by Interpal in the 1996 and 2003 inquiries.<sup>25</sup> In September 2006 a federal judge in New York denied NatWest’s motion to dismiss the suit, allowing it to continue.<sup>26</sup>

### **Tamils Rehabilitation Organisation (2000-2005)**

In September 2000, the Charity Commission opened an Inquiry into the Tamils Rehabilitation Organisation (TRO), after allegations that TRO was “supporting terrorist activity by transferring funds to Sri Lanka in support of the Liberation of Tamil Tigers of Elam (LTTE),” a proscribed organization under the U.K. Terrorism Act 2000 and under many other nations’ laws as well. TRO worked by providing funds to the Tamils Rehabilitation Organisation Sri Lanka (TRO SL), and it appeared that some of those funds might be making their way to the Tigers.

After receiving information that the charity’s “funds might be at risk,” the Commission restricted payments from TRO accounts under section 18 of the Charities Act (a step short of a complete freeze on the use of assets), and then found inadequate financial controls, lack of operational transparency, and evidence of mismanagement during its investigation. “The Trustees exercised little or no control over the application of funds in Sri Lanka and failed to demonstrate a clear audit trail relating to expenditure. They also failed to provide the Commission with any explanation as to the provenance of some of the funds received from the US and Canada. The Commission therefore concluded that the Charity’s property was at risk,” and appointed a prominent London lawyer as TRO’s interim manager under the Charities Act.

The interim manager’s tasks were indeed broad – in addition to managing the entire charity, he was charged with “establishing whether it was able to operate lawfully, in the manner intended by the Trustees, in providing charitable relief to Sri Lanka in circumstances of civil unrest” “and “required to ascertain the extent of the risk that funds had been, or

<sup>25</sup> Victims of Bombings in Israel Seek Damages in New York, *New York Times*, 7 January 2006; Hurt by Hamas, Americans Sue Banks in U.S., *New York Times*, 15 April 2006.

<sup>26</sup> NatWest Loses First Round in Court Case over Charity Linked to Hamas, *The Guardian* (London), 29 September 2006.

would in the future be, received by any organisation proscribed..." and "making recommendations for the Charity's future."

The interim manager, Don Bawtree of BDO Stoy Hayward, determined that the Trustees could not account for funds and "were not administering the charity to an acceptable standard." He commissioned a Sri Lankan firm to trace funds from TRO to TRO SL and onward to charitable activities in Sri Lanka, and that investigation determined that "TRO SL liaised with the LTTE in determining where funds could be applied." Funds donated "were used for a variety of projects which appeared to be generally humanitarian, but not necessarily charitable in English law nor in line with the Charity's objects." The manager sought to find an NGO willing to work with TRO in finding appropriate projects and monitoring them effectively, but could not find an NGO willing to take this task on.

The interim manager then set up a separate new charity, the Tamil Support Foundation, in which he and the Commission could have confidence that legal obligations were being met. The plan was to transfer funds from the TRO to this new charity. (This seemingly extraordinary power is contemplated in the Commission's authorizing legislation and appears to be unquestioned in Britain.) Then the tsunami hit Sri Lanka and other countries in December 2004, and the manager decided to donate most of TRO's assets to tsunami relief through recognized charities, as well as to transfer some funds to the new Tamil Support Foundation. By August of 2005 TRO had no funds left because they had all been transferred to legitimate organizations working on tsunami relief or to the new, safeguarded Tamil Support Foundation. TRO ceased to operate, it was removed from the Register of Charities, and the Commission discharged the interim manager.

From the perspective of the Commission, the results of this long and complex process were entirely positive: "The appointment of the Interim Manager protected the Charity's funds at the time when he took control of its bank accounts, by preventing them from being applied in a manner that was unaccountable....Through the setting up of the Tamil Support Foundation, the Interim Manager secured another vehicle for those wishing to support the Tamil speaking people."<sup>27</sup>

---

<sup>27</sup> All quotations in this section are from Charity Commission, Inquiry Report: Tamils Rehabilitation Organisation, 2005 ([www.charity-commission.gov.uk/investigations/inquiryreports/tamils.asp](http://www.charity-commission.gov.uk/investigations/inquiryreports/tamils.asp)).

## New Initiatives Against Terrorist Financing through Charities, 2006

The July 2005 bombings in London and charges of other links between British-based charities and terrorists abroad have brought renewed pressure to clamp down on terrorist networks and their financing. Intelligence and police activities, raids and detentions have increased dramatically, and the British government has proposed new measures on terrorist finance that could well affect the charitable sector in the U.K. And the U.K. is under continuing, perhaps increasing pressure from other countries – including the U.S., Israel, Russia and others – to control terrorist finance through charities.

In February 2006 the United Nations added several more individuals resident in the United Kingdom, three companies and a related charity based in Birmingham, the Sanabel Relief Agency, to its list of internationally proscribed individuals and groups linked to terrorism. Sanabel and the individuals and companies were allegedly linked to an al-Qaeda-affiliated group called the Libyan Islamic Fighting Group.<sup>28</sup> The Charity Commission immediately opened an investigation as well and, it became clear later, British authorities either began or continued intensive surveillance of the group.

In February 2006, Gordon Brown MP announced that the government would conduct a new review of measures to combat the use of charities in terrorist finance and would establish a new intelligence center to investigate terrorist financing networks around the world and their impact on Great Britain. “[C]ut[ting] off the sources of terrorist finance ... requires an international operation using modern methods of forensic accounting as imaginative and pathbreaking for our times as the Enigma codebreakers at Bletchley Park achieved more than half a century ago.” At the same time, the government announced that it had frozen 80 million pounds of terrorist funds since September 2001 involving more than a hundred organizations.<sup>29</sup>

In May, more than 500 British police raided nineteen locations around England in London, Bolton, Birmingham, Middlesbrough, Liverpool and Manchester against individuals and organizations suspected of

---

<sup>28</sup> Man Denies Terror Link after Assets Freeze, *The Guardian* (London), 9 February 2006.

<sup>29</sup> Modern-Day Bletchley Park to Tackle Terror Finance Networks, *The Guardian* (London), 11 February 2006.

funneling financial assets to terrorist organizations abroad. "At the center of the raids," according to *The Guardian*, was Sanabel, whose offices were entered and one of whose trustees, Tahir Nasuf, was arrested under the Terrorism Act 2000.<sup>30</sup>

Also in May, Israel called the British-based charity Islamic Relief a "front for terrorists" involving the "transfer [of] funds and assistance to various Hamas institutions and organizations." The charges raised bilateral issues between Israel and Great Britain because Britain finances Islamic Relief's health and other work in Gaza and elsewhere. Islamic Relief denied the charges and said that Israel appeared to have confused several of its sub-grantees with groups tied to Hamas. And the U.K. government overseas aid group that funded Islamic Relief, the Department for International Development, said "[w]e have no reason to believe that the allegations are true."<sup>31</sup>

In the summer of 2006, after British authorities uncovered a plot to blow up airliners traveling between Britain and the United States and detained 25 people, a British-based charity called Jamaat ud Dawa (Association of the Call to Righteousness) and a smaller, family-run charity named Crescent Relief came under investigation for possible diversion of earthquake relief funds to terrorist groups that had planned to carry out the airliner attacks. The funds were reported to have come directly from the British organization or individuals linked to it.

News reports linked Jamaat ud Dawa – which is on the U.S. proscription lists – to Lashkar-e-Taiba, a terrorist group banned by both the U.S. and Pakistan. New reports made clear that Jamaat ud Dawa and individuals linked to it had been under intensive surveillance for some time. A Charity Commission investigation was immediately launched as well, with its focus on Crescent Relief.<sup>32</sup>

---

<sup>30</sup> Ten Held in Police Counter-Terror Raids Over Claims of Chanelling Cash to Iraq Insurgency, *The Guardian* (London), 25 May 2006.

<sup>31</sup> Israel Accuses British-funded Islamic Charity of Being Front for Terrorists, *The Guardian* (London), 31 May 2006.

<sup>32</sup> Pakistani Charity Under Scrutiny in Financing of Airline Bomb Plot, *New York Times*, 14 August 2006; Terror Plot, *The Guardian* (London), 15 August 2006; In British Inquiry, a Family Caught in Two Worlds, *New York Times*, 20 August 2006; Arrest: Father of Airline Attack Suspects is Held in Pakistan, *The Guardian* (London), 21 August 2006; British Study Charitable Organization for Links to Plot, *New York Times*, 25 August 2006; In Tapes, Receipts and a Diary, Details of the British Terror Case, *New York Times*, 28 August 2006.



All these events sparked more intensive focus on charitable links to terrorism and their role in terrorist finance, especially links involving Islamic charities. As the *New York Times* reported from London in August, “the question is being asked here, with more urgency: To what extent to Muslim charities – on the surface noble and selfless – mask movements and money for terrorists and extremist groups?” And events in 2005 and 2006 highlighted the different approaches – in some cases divergent approaches – taken by American and British authorities on terrorist finance and on charities that had come under suspicion.

“Since Sept. 11,” the *Times* continued, “American officials have banned many charities that still operate freely in Britain, reflecting a disagreement about where charity ends and extremism begins.” And increasingly American officials and commentators were critical of the process-based British approach, calling the Charity Commission and other British institutions “too lax.” All agreed that “the British showed signs of hardening, particularly after four bombers killed 52 people on buses and trains here on July 7 of last year.”<sup>33</sup>

In the wake of the airline bomb plot arrests, the government reconfirmed that the Home Office and Treasury Department are reviewing the problem of terrorist finance through charities and intend to recommend legal and policy changes. “We are aware that existing safeguards against terrorist abuse in the charitable sector need to be strengthened,” a Home Office official told the *New York Times*.<sup>34</sup> The National Council of Voluntary Organizations (NCVO) also convened a panel to report on issues of charities and terrorist finance, concerned that the Home Office and security review would not be sufficiently consultative.

The investigations continued into the fall, including a widespread investigation of alleged “jihadists” that culminated in the arrest of fourteen people in London in September. They had allegedly been training for terrorist activities, including possibly at an independent school owned and run by the charitable group Jameah Islamiyah, which came under investigation by the Charity Commission as well in the fall of 2006.<sup>35</sup>

---

<sup>33</sup> Airplane Terrorism Case Prompts Questions About the Work of Islamic Charities in Britain, *New York Times*, 24 August 2006.

<sup>34</sup> British Study Charitable Organization for Links to Plot, *New York Times*, 25 August 2006.

<sup>35</sup> Police Search Islamic School on Expansive Estate in South Britain, *New York Times*, 4 September 2006; Training Camps Link to Anti-Terror Arrests, *The Guardian* (London), 4 September 2006.

In October, the government began announcing some of its new measures to crack down on terrorist financing. Chancellor Gordon Brown and Economic Secretary Ed Balls stressed “closer cooperation between America and Europe,” and said that the U.K. government would now “use classified intelligence to freeze assets of those suspected of having links to terrorism” and “allow law enforcement agencies to keep their sources of information secret after it is used to track down and freeze bank accounts.” The government would also seek preemptive authority to halt terrorist financing. The inquiry on charities and terrorist finance continued. Brown also proposed new and inevitably controversial reforms to Britain’s terrorist law, including giving the government the power to detain terrorist suspects for longer than the current 28 days.<sup>36</sup>

The Terrorism Act 2006 adds to the array of counter-terror enactments in the U.K. since September 11, particularly the Terrorism Act 2000 and the Anti-Terrorism, Crime and Security Act 2001. It may affect charities because it expands the terrorist criminal offenses to include acts preparatory to terrorism; directly or indirectly inciting or encouraging others to commit terrorism, including the “glorification” of terrorism; the sale, loan or other dissemination of publications that encourage terrorism or provide assistance to terrorists; and anyone who gives or received training in terrorist techniques, including mere attendance at a terrorist training site. The Terrorism Act 2006 also increases the scope of proscription for terrorist organizations, providing the government with authority to proscribe organizations that “glorify terrorism.”<sup>37</sup>

As of fall 2006, 42 organizations had been proscribed in the U.K. under the Terrorism Act 2000, 14 organizations were proscribed in Northern Ireland under earlier law, and under the new authority given to proscribe organizations that glorify terrorism in the Terrorism Act 2006, two such organizations had been banned.<sup>38</sup>

In January 2007 NCVO released its report on charities and terrorist finance, titled *Security and Civil Society*. The report strongly criticized

---

<sup>36</sup> U.K. Unveils Plan to Freeze Terror Funds, Associated Press, 10 October 2006; Brown to Use Classified Intelligence in Fight to Cut Terrorist Funding, *The Guardian* (London), 11 October 2006.

<sup>37</sup> Home Office, Counter-Terrorism Strategy, Terrorism Act 2006 ([security.homeoffice.gov.uk/counter-terrorism-strategy](http://security.homeoffice.gov.uk/counter-terrorism-strategy)).

<sup>38</sup> Home Office, Counter-Terrorism Strategy ([security.homeoffice.gov.uk/counter-terrorism-strategy](http://security.homeoffice.gov.uk/counter-terrorism-strategy)); Home Secretary Moves to Ban 15 Terror Groups, Home Office, Press Office, 10 October 2005 (press. [homeoffice.gov.uk/press-releases](http://homeoffice.gov.uk/press-releases), containing a full banning order and additional information).

moves toward strengthening the UK legal regime for prosecuting charities and called on the government to view charities as an ally in the fight against terrorism rather than as an adversary. The report also pointed out the fundamental sufficiency of the existing legal regime while also recognizing some problems, and it criticized the impact of some government actions in this arena on charitable activities in the UK and abroad, particularly with respect to Muslim organizations.<sup>39</sup> The awaited Home Office and security review of charities and terrorist finance is expected to be released in February 2007.

## **Lessons of the Experience in the United Kingdom**

The English experience shows the value of continuing to have sophisticated charity regulators play a central role in investigating charitable links to terrorism and terrorist finance, including maintaining legal authority over these issues in the charity regulator. The Charity Commission has played an exceptionally useful role in England in cooperation with police and security forces, bringing to bear a detailed knowledge of the sector and of individual charitable organizations based on years of reporting and experience. The Charity Commission conducts investigations, gathers information that it shares as relevant with other agencies, and may take measures to require organizations to substitute trustees, improve accounting and disbursement, or other reforms.

This maintenance of a central role for a charity regulator, combined with the intensive focus on a small number of organizations suspected of terrorist finance links, has arguably resulted in both better targeting and better information for British law enforcement than for some of its international counterparts. The British situation contrasts with Australia, where anti-terrorism laws have been adopted that clearly could apply to the charitable sector, but have not yet been applied, and with the U.S. prosecution-centered approach. The approach taken in the United States and Australia will be discussed below.

---

<sup>39</sup> NCVO, Security and Civil Society (January 2007) ([www.ncvo-vol.org.uk](http://www.ncvo-vol.org.uk)).

### III. United States

#### The Framework of Anti-Terrorist Law and Policy

In the United States, enhanced regulation of charitable ties to terrorism (usually reflecting concerns about terrorist financing) goes back to the 1993 bombing of the World Trade Center, including legal provisions that allow proscription of terrorist organizations and that bar material support to terrorist organizations. These provisions have been the subject of extensive litigation in the United States and have generally been upheld.

By the time of the September 2001 attacks, a fairly comprehensive legal framework for investigating and prosecuting charitable links to terrorism was in place. In particular, the Antiterrorism and Effective Death Penalty Act, adopted in 1996, criminalized “material support” for terrorist organizations through charitable and other vehicles. The International Emergency Economic Powers Act (“IEEPA”), originally enacted in 1977, also prohibits transactions that the Executive Branch has determined to be inimical to the national security of the United States, including terrorist financing through charities.

These pre-2001 statutes were supplemented almost immediately after September 11 by Executive Order 13224 (October 2001), which eased the process of proscription and freezing of terrorist assets, and by several of the provisions of the Patriot Act (November 2001), which were made applicable to the charitable sector. Among its provisions, the Patriot Act expanded the ability of the government to seize assets of “persons engaged in planning or perpetrating ... terrorism,” or “acquired or maintained” for that purpose, or “derived from [or] involved in terrorism.” The Patriot Act also barred “expert advice or assistance” to designated terrorist organizations, a bar that has been applied to charitable organizations and has been the subject of extensive litigation. Such provisions are of course applicable to charitable and nonprofit institutions as well as a much broader range of individuals and organizations.<sup>40</sup>

The government’s first moves in this area were against several Muslim charities, initially the Benevolence International Foundation, Global Relief Foundation, and the Holy Land Foundation for Relief and Development.

---

<sup>40</sup> For further information, see Sidel, *More Secure, Less Free?*, chapter 6.



Each was closed and their assets frozen in late 2001 and after on charges of violating the prohibition against providing “material support and resources” to a foreign terrorist organization, as well as violations of the IIEPA, money laundering, tax evasion, and other charges.

The government’s offensive against several Muslim charities was pursued with a vigor that convinced many in the American nonprofit sector that the government’s actions were based on solid evidence. But in the heat of the environment after the horrendous and murderous attacks of September 2001, the remainder of the American nonprofit sector generally did not consider it an option to criticize the breadth of government tactics in the investigation and closure of Muslim charities that admittedly distributed funds in the Muslim world and, admittedly, in some cases to terrorist organizations and the families of suicide bombers.<sup>41</sup>

Some, however, tried to indicate problems with the breadth and potential implications of government’s approach. Key Muslim community organizations warned that the government’s actions contributed to an anti-Muslim backlash. But outside the Muslim community, there were few dissenting voices. One of the few was the director of an umbrella association of nonprofits in Ohio, in the American industrial midwest. This nonprofit leader stepped forward in 2002 to warn of the quote “implications of the unprecedented effort by federal agencies, working in concert, to shut down significant charities, seize their records and assets, and force the organizations to suspend operations until their innocence can be proven.”<sup>42</sup>

But those voices were solitary ones. Most of the nonprofit sector in the United States hoped for a kind of unspoken bargain with the government: government criminal enforcement would be limited to Muslim charities that had funneled donations to some combination of terrorist and charitable activities abroad, and those organizations would be considered guilty until proven innocent. Meanwhile, in the other side of this unspoken bargain, the rest of the American nonprofit sector seemed to hope that the broader sector would remain unaffected, undisturbed by the investigations, indictments and broad statements about a group of registered Muslim charities, nor the possibility that the new Patriot Act could be applied vigorously against the nonprofit sector well beyond a handful of Muslim charities.

---

<sup>41</sup> These prosecutions are discussed in more detail in Sidel, *id.*

<sup>42</sup> Richard Moyers, A Shocking Silence on Muslim Charities, *Chronicle of Philanthropy*, 17 October 2002.

The director of the Ohio nonprofit association challenged that unspoken bargain. "Will any organization be subject to the same treatment if the government claims links to terrorism? How broadly will terrorism be defined .... ? What about eco-terrorism, or domestic disruptions such as the protests organized against global trade and financial institutions? If a major U.S. philanthropic institution is discovered to have made a grant to an organization that the government claims is linked to terrorism, will it be subject to the same 'seize and shut-down' treatment?"<sup>43</sup>

In late 2002, however, the U.S. administration took a broader action that more deeply concerned a wider range of the American philanthropic and nonprofit sector.

That step was the release of the *Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-based Charities*, by the U.S. Treasury Department in late 2002. The Guidelines provided a broad and detailed range of new provisions for charitable and philanthropic organizations to use in their overseas giving, intended to prevent the channeling or diversion of American funds to terrorist organizations or purposes. These steps included the collection of considerably more information about grantees than is often available, the vetting of grantees, extensive donor review of financial operations beyond industry norms, and other requirements in quite detailed terms.<sup>44</sup>

In the words of Barnett Baron, Executive Vice President of the Asia Foundation, the 2002 Treasury Guidelines carried the danger of "setting potentially unachievable due diligence requirements for international grant-making, [and] subjecting international grant-makers to high but largely undefined levels of legal risk, [which] could have the effect of reducing the already low level of legitimate international grant making."<sup>45</sup>

When threatened by government action that many prominent public charities active in overseas aid and foundations considered overbroad, vague, and impossible to implement effectively, a significant portion of

---

<sup>43</sup> Id.

<sup>44</sup> U.S. Treasury Department, *Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-Based Charities*, November 2002.

<sup>45</sup> Barnett Baron, *Deterring Donors: Anti-Terrorist Financing Rules and American Philanthropy*, *International Journal of Not-for-Profit Law* 6(2), 1-32 (2004).

the American philanthropic and nonprofit community providing aid and support overseas began to act, complaining about the breadth of the government's so-called "voluntary" prescriptions. A band of major charities and foundations, angered and anxious at the sweep of the Treasury's new guidelines and fearful that "voluntary best practices" would be treated as law even though they had not been adopted by Congress or formally adopted by a government agency, sought to engage the U.S. Treasury in discussions on the Anti-Terrorist Financing Guidelines. After lengthy discussion, these foundations and charities active overseas also proposed a new approach: what it called the *Principles of International Charity*.

They prefaced their new Principles by noting that "after consideration of both the effectiveness of existing procedures and the implications of strict compliance with the [Anti-Terrorist Financing] Guidelines, charitable organizations concluded that Guidelines are impractical given the realities of international charitable work and unlikely to achieve their goal of reducing the flow of funds to terrorist organizations, but very likely to discourage international charitable activities by U.S. organizations." The nonprofits asked the government to withdraw the onerous and ineffective Treasury Department Guidelines and to substitute the new *Principles of International Charity* drawn up by the nonprofit and philanthropic sector.<sup>46</sup>

Those *Principles of International Charity* emphasized compliance with American law but also that charitable organizations and foundations are not agents of the U.S. government. They emphasized that charities are responsible for ensuring, to the best of their ability, that charitable funds do not go toward terrorist organizations, and that there are key baseline steps that can be taken to help in reaching that goal – but also that there are a diverse range of ways to accomplish that goal, and that different methods of safeguarding and protection will work for different kinds of organizations that have different types of risk. And the charitable organizations concluded, "each charitable organization must safeguard its relationship with the communities it serves in order to deliver effective programs. This relationship is founded on local understanding and acceptance of the independence of the charitable organization. If this foundation is shaken, the organization's ability to be of assistance and the safety of those delivering assistance is at serious risk."<sup>47</sup>

---

<sup>46</sup> Principles of International Charity (developed by the Treasury Guidelines Working Group of Charitable Sector Organizations and Advisors, March 2005) ([www.independentsector.org/programs/gr/CharityPrinciples.pdf](http://www.independentsector.org/programs/gr/CharityPrinciples.pdf)). In effect, the organizations sought to convince the authorities that a self-regulatory approach would work better in controlling these matters.

<sup>47</sup> Id.



In response to the charitable and philanthropic sector's concern, and because of the unworkability of the earlier, hastily drafted Guidelines, the Treasury revised its Guidelines on overseas giving in December 2005. The "revised" *Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-Based Charities* did make some improvements, particularly in reducing some of the onerous and unworkable due diligence burdens on American organizations providing charitable funds overseas.<sup>48</sup>

But three basic issues remained that were of continuing and deep concern to the nonprofit sector. First, in the words of the concerned charities and foundations, "the revised Guidelines contain provisions that [continue to] suggest that charitable organizations are agents of the government." Such an assumption could lead both to declining effectiveness and to severe harm to American aid personnel working overseas. Second, the revised Guidelines seem to require nonprofits funding overseas to collect even more data than the original 2002 Guidelines would have required. And third, the nonprofit community remained deeply concerned that these so-called "voluntary best practices" were in fact stealth law, adopted without consideration by Congress or formal rulemaking by an agency. In the words of the concerned charities and foundation Working Group, "we are concerned that the revised Guidelines will evolve into de facto legal requirements through incorporation into other federal programs, despite the inclusion of the word "voluntary" in the title."<sup>49</sup>

When directly confronted with government action that would impinge on the ability of American nonprofits and foundations to undertake overseas giving and perhaps endanger their programs, the American nonprofit and philanthropic sector began to resist aspects of the new government regulation of the nonprofit sector based in anti-terrorism. A battle of sorts has been joined between the government and the philanthropic sector concerning overseas giving, and neither side is giving in: The Treasury has not withdrawn the new, revised Guidelines on overseas giving (and in fact re-revised those in late 2006),<sup>50</sup> and the nonprofit community continues

---

<sup>48</sup> U.S. Treasury Department, *Revised Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-Based Charities* (2005) ([www.treas.gov/offices/enforcement/key-issues/protecting/charities-intro.shtml](http://www.treas.gov/offices/enforcement/key-issues/protecting/charities-intro.shtml)). This approach means, perhaps ironically, that legitimate and well-meaning charities will struggle to comply with standards while less professional or less well-meaning groups may not, as Professor Kent Roach has pointed out to me.

<sup>49</sup> Council on Foundations, Letter to the U.S. Treasury Department on the Revised Anti-Terrorist Financing Guidelines (2006) ([www.usig.org/PDFs/Comments\\_to\\_Treasury.pdf](http://www.usig.org/PDFs/Comments_to_Treasury.pdf)).

<sup>50</sup> See [http://www.ustreas.gov/offices/enforcement/key-issues/protecting/docs/guidelines\\_charities.pdf](http://www.ustreas.gov/offices/enforcement/key-issues/protecting/docs/guidelines_charities.pdf).



to insist that its Principles of International Charity should be substituted for the government's revised Guidelines. But this only occurred when the sector saw itself as directly threatened.

In 2005 and 2006 the fallacy of assuming that government actions would be directed solely against a few Muslim charities, and that the remainder of the nonprofit sector would be left alone, has been further challenged by the emergence of new evidence indicating that my government has, in fact, targeted a much broader swathe of the American nonprofit sector for surveillance and observation. It is now clear that literally hundreds or even thousands of American nonprofits have had events observed, telephone calls sorted, or financial transactions examined by government agencies.<sup>51</sup> And in early 2007 it was also revealed that the U.S. government is employing donor-tracking software to search and correlate donors to an as-yet undefined range of nonprofit institutions.<sup>52</sup>

These developments have had other unfortunate consequences as well. In particular, American foundations have been deeply concerned about potential investigations of their grant making by the executive or legislative branches, and several have responded by shifting responsibility to their grantees, through new and broadly worded grant letters, not to engage in any activity that might be considered redolent of bigotry or encouraging terrorism or violence. The Ford Foundation has been particularly active in this area, arising out of its disgust with the anti-Semitic statements made by one of its grantees at the United Nations Conference on Racism in Durban in 2000. But the breadth of the prohibitions in its new grant letters prompted opposition from a group of elite universities and a decision by the American Civil Liberties Union not to sign the broad new grant letter provisions and thus not to accept new funds from Ford,<sup>53</sup> a sharp response to the self-regulatory (and defensive) approach that Ford had adopted.

After negotiations between the Ford Foundation and a number of universities, the Foundation reaffirmed its commitment to academic

---

51 MSNBC, *Is the Pentagon Spying on Americans? Secret Database Obtained by NBC News Tracks 'Suspicious' Domestic Groups*, [MSNBC.com](http://MSNBC.com) (NBC News), 14 December 2005; Surveillance Net Yields Few Suspects, *The Washington Post*, 5 February 2006.

52 Anti-Terrorism Program Mines IRS Records; Privacy Advocates are Concerned that Tax Data and Other Information May Be Used Improperly, *Los Angeles Times*, 15 January 2007.

53 Sidel, *More Secure, Less Free?*, id.; S. Sherman, Target Ford, *The Nation*, 5 June 2006.

freedom and free speech on campus, making clear that the language in the grant letter was not intended to interfere with academic freedom and free speech. In at least one case – Stanford – where the institution remained wary of signing the Foundation’s very broad language, a “side letter” was issued to that institution recommitting Ford in strong terms to academic freedom and free speech.<sup>54</sup>

But this issue affected others as well. In 2004, after extensive internal debate, the American Civil Liberties Union also began declining Ford Foundation and Rockefeller Foundation grants. The ACLU did so, in the words of its Executive Director, Anthony Romero, “rather than accept restrictive funding agreements that might adversely affect the civil liberties of the ACLU and other grantees” by restricting the free speech rights of the ACLU and its members. The ACLU issued a statement that primarily blamed the government, not the Ford Foundation, for this conflict:

“This administration and its war on terror have created a climate of fear that extends far beyond national security concerns and threatens the civil liberties of all Americans.... The board and leadership of the ACLU have made the painful but principled decision to turn down \$1.15 million in future funding from the Ford and Rockefeller Foundations rather than accept restrictive funding agreements that might adversely affect the civil liberties of the ACLU and other grantees.... It is a sad day when two of this country’s most beloved and respected foundations feel they are operating in such a climate of fear and intimidation that they are compelled to require thousands of recipients to accept vague grant language which could have a chilling effect on civil liberties. But the ambiguities are simply too significant to ignore or accept. They include potential prohibitions on free speech and other undefined activities such as “bigotry”

---

<sup>54</sup> For a detailed account of Stanford’s discussions with Ford from the Stanford perspective, see the January 26, 2005 minutes of the Stanford Faculty Senate at [news-service.stanford.edu/news/2005/January26/minutes-012605.html](https://news-service.stanford.edu/news/2005/January26/minutes-012605.html).

as part of a misconceived war on terror. Indeed, vague terms such as “bigotry” often have charged meanings in a post-9/11 world. The ACLU cannot effectively defend the rights of all Americans if we do not stand up for those same rights ourselves....”<sup>55</sup>

This was a remarkable break. The Ford Foundation and the ACLU have a long and close history of work, and Ford has provided millions of dollars in grants to the ACLU for programs, operating costs, and endowment. As the President of the Ford Foundation, Susan Berresford, put it in a subdued statement in which Ford’s respect for the ACLU was fully clear.

“We share the same basic values as the ACLU. The ACLU is dedicated to defending free speech, and we fully support their work in doing so. We also fully support their work in defending the rights of promoters of unpopular causes. That is why we have provided significant general financial support to the organization over the years for the full range of its activities.....The issue at hand has to do with our different missions. Ford’s mission is to strengthen democratic values, reduce poverty and injustice, promote international cooperation and advance human achievement. Consistent with that mission, we are proud to support the ACLU’s defense of free speech. We do not, however, believe that a private donor like Ford should support all speech itself (such as speech that promotes bigotry or violence). We accept and respect the fact that we have a different mission from the ACLU, even while we share the same basic values....We hope that over time we will once again work together.”<sup>56</sup>

---

<sup>55</sup> See ACLU Declines Ford and Rockefeller Grants Due to Restrictive Funding Agreement; Painful but Principled Decision to Put Civil Liberties First, Statement of Anthony D. Romero, ACLU Executive Director, October 17, 2004, at [www.aclu safefree/general](http://www.aclu safefree/general).

<sup>56</sup> Statement of Susan V. Berresford in response to announcement by the American Civil Liberties Union, [www.fordfound.org/news/view\\_news\\_detail.cfm?news\\_index=147](http://www.fordfound.org/news/view_news_detail.cfm?news_index=147).

In another related step, during the summer of 2004 the federal agency that runs the Combined Federal Campaign – the integrated giving effort for hundreds of thousands of federal employees in which government workers donate to nonprofit – announced a significant change in its policies. The agency issued a memorandum requiring each nonprofit receiving CFC funds to certify that it “does not knowingly employ individuals or contribute funds to organizations found on the ... terrorist related lists promulgated by the U.S. Government, the United Nations, or the European Union.” The new, mandatory certification requirement was explicitly drawn from the provisions of the so-called “voluntary” anti-terrorism financing guidelines issued by the Treasury Department in 2002.<sup>57</sup>

This new requirement ignited a firestorm of controversy. A number of American nonprofit organizations refused to sign the certification, arguing that they could not vouch for every single one of their employees, contractors, consultants and anyone else who worked with their organizations, particularly given the chaotic nature of the government’s terrorist watch lists. Finding such a name, though clearly a false positive, would require nonprofits to ask the employee “intrusive questions about his [or her] personal life and beliefs.”<sup>58</sup> They argued that the federal agency administering the Combined Federal Campaign lacked the statutory or Constitutional authority to issue this new regulation, and that doing these kinds of checks would violate the privacy and associational rights of their employees. And they opposed the conversion of the so-called “voluntary” guidelines issued by the Treasury Department into a legal mandate without Congressional approval or formal rulemaking.<sup>59</sup>

Eventually the American Civil Liberties Union and a number of other organizations filed suit against the federal government seeking to overturn the new certification requirement.<sup>60</sup> In the meantime, nonprofits lost funds because of their refusal to sign the certification – the ACLU, for

---

<sup>57</sup> Combined Federal Campaign, Combined Federal Campaign Memorandum 2003-10, New Certification for 2004 CFC Application (2003) ([www.opm.gov/cfc/opmmemos/2003/2003-10.asp](http://www.opm.gov/cfc/opmmemos/2003/2003-10.asp)).

<sup>58</sup> American Civil Liberties Union, ACLU Announces Diverse Nonprofit Coalition Opposing Restrictions on Recipients of the Combined Federal Campaign, 12 August 2004 ([www.aclu.safefree/general](http://www.aclu.safefree/general)).

<sup>59</sup> ACLU to Withdraw from Charity Drive, *New York Times*, 1 August 2004; Nonprofits Scramble to Meet Terror Rules; Worker Screening Required for CFC funds, *Washington Post*, August 14, 2004; see also Sidel, *More Secure, Less Free?*, id.

<sup>60</sup> Charities Sue Over Antiterrorism Certification Regulation, *New York Times*, 11 November 2004; Groups Sue OPM on Terrorism Rule; Charities Told to Screen Workers, *Washington Post*, 11 November 2004.



example, lost \$500,000 in donations by federal government employees in 2005.<sup>61</sup> In November 2005, however, the federal government withdrew the new requirement that recipient organizations under the Combined Federal Campaign sign the certification in favor of a much more general pledge by organizations participating in the Combined Federal Campaign that they are in compliance with existing anti-terrorist financing laws.<sup>62</sup>

The prosecutions of Benevolence, Global Relief and Holy Land were pursued over several years and in several cases remain under prosecution. They represent a different approach from the Charity Commission-based British approach that contemplates correction of wrongdoing, intermediate steps and sanctions, and, at least at times, attempts to differentiate charitable funds flowing to terrorist activities from charitable funds flowing to humanitarian activities. And the “material support” prohibition, in particular, has sparked extensive litigation in the United States that remains uncompleted.

### **Summary of U.S. Law, Policy and Impact**

The U.S. government has favored a prosecution-driven approach, often based on strict or negligence liability as opposed to specific intent, in contrast to the more “regulatory” approach of the British authorities and the Charity Commission, though the Treasury’s voluntary guidelines do represent a supplement to a purely prosecutorial approach. At the same time, unofficial guidelines, such as the Treasury’s guidelines on overseas giving, were drafted hastily, without sufficient consultation, and in such broad terms as to overreach, have little effect on actual terrorist finance, and even harm American charitable work abroad. In turn government agencies (such as the Combined Federal Campaign) and grantmaking organizations (such as the Ford Foundation) employ the approach pioneered by the government in shifting risk downward – to grantee organizations in both cases.

---

<sup>61</sup> ACLU Board is Split Over Terror Watch Lists, New York Times, 31 July 2004.

<sup>62</sup> Requirement on Watch Lists is Dropped, New York Times, 10 November 2005.

### III. Australia

#### The Framework of Anti-Terrorist Law and Policy

In contrast with the United Kingdom and the United States, Australia had very little experience with terrorism within its borders before the September 11 attacks and thus very little specifically anti-terrorist legislation on its books.<sup>63</sup>

After the September 11 attacks, the government tightened domestic surveillance of suspected terrorists and introduced a number of anti-terrorism bills in the Australian parliament that, in general terms, sought to enhance government power in the anti-terrorism arena by vesting additional discretion and power in the Australian federal attorney general. Those bills included the Security Legislation Amendment (Terrorism) Bill, Suppression of the Financing of Terrorism Bill, Criminal Code Amendment (Suppression of Terrorist Bombings) Bill, Border Security Legislation Amendment Bill, and Telecommunications Interception Legislation Bill, all introduced in 2002.<sup>64</sup>

The initial legislative proposals elicited widespread and broad opposition in Australia, including civil liberties groups and parliamentarians who argued that much of what the government wanted to re-criminalize through specialized anti-terrorist legislation was already effectively criminalized and handled through existing criminal law.<sup>65</sup> Opponents forced some changes in the original set of bills adopted in the wake of the September 11 attacks. The very broad proposed definition of “terrorist act” in the government’s initial proposal was narrowed to require some element of intentional intimidation or coercion. And the government’s attempt to reverse the presumption of innocence in terrorism cases, requiring detainees to prove that they were not terrorists, was corrected.

---

<sup>63</sup> Christopher Michaelsen, International Human Rights on Trial: The United Kingdom’s and Australia’s Legal Response to 9/11, 25 *Sydney Law Review* 275-303 (2003). An earlier and shorter treatment of the Australian scene is in Sidel, *More Secure, Less Free?: Antiterrorism Policy and Civil Liberties after September 11* (University of Michigan Press, 2004, and 2006 revision).

<sup>64</sup> David Kinley and Penny Martin, International Human Rights Law at Home: Addressing the Politics of Denial, 26 *Melbourne University Law Review* 466-77, 471 (2002).

<sup>65</sup> For a clear expression of this view, see, e.g., Chris Maxwell, September 11 and Its Aftermath: Challenges for Lawyers and the Rule of Law (Address to Maddock Lonie and Chisholm law firm, 15 April 2002) ([www.libertyvictoria.org.au/documents/2002-04-15\\_cm\\_speech.pdf](http://www.libertyvictoria.org.au/documents/2002-04-15_cm_speech.pdf)).

The initial wave of legislative activity continued in 2003, when the government proposed the Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003 (the ASIO Act), which was primarily intended to enable Australian security organisations to detain terrorism suspects or persons who might have some knowledge of potential terrorist activities and to criminalize “withholding of information regarding terrorism.”<sup>66</sup> This bill also elicited very strong opposition, delaying passage for more than a year, and resulting in softening to protect children in detention, add a sunset clause, and other changes.

In 2003 and 2004 the government continued to press for statutory amendments to provide for closed trials for defendants charged with national security offenses, and clearances for lawyers, limited public access, and limited media coverage of certain national security trials, as well as authority to deny terrorism suspects bail and allow police to hold some detainees for terrorism-related questioning for twenty-four hours, a substantial increase from the four hour limit under current law.<sup>67</sup>

In 2005 the Australian government proposed new and tougher anti-terrorism legislation that would expand the definition of terrorist organizations to include advocacy within the proscribable range, expand the government’s powers to use “control orders” and preventive detention against a widened range of suspects, and strengthen the crime of sedition.<sup>68</sup> The proposed expansion in government powers continued to be severely criticized by civil liberties groups.<sup>69</sup>

## Charities and Terrorist Finance

Within the framework of new and expanded anti-terrorist lawmaking in Australia there has been some attention to the problem of terrorist finance – and within that rubric, some, but not extensive, attention to the issue of charitable conduits for terrorist finance. Among the laws passed in 2002 was the Suppression of the Financing of Terrorism Act 2002, which was intended to provide Australian implementation of the International

<sup>66</sup> Michaelsen, International Human Rights on Trial, *supra* note 8, p. 281

<sup>67</sup> These developments are discussed more fully in Sidel, *More Secure, Less Free*, pp. 156-62.

<sup>68</sup> See Prime Minister’s Officer, Counter-Terrorism Laws Strengthened, 8 September 2005 at [www.pm.gov.au](http://www.pm.gov.au); Civil Rights Network, The Anti-Terrorism Bill (No 2) 2005 (Cth), [www.civilrightsnetwork.org](http://www.civilrightsnetwork.org). The text of the draft is at [www.chiefminister.act.gov.au/docs/B05PG201\\_v281.pdf](http://www.chiefminister.act.gov.au/docs/B05PG201_v281.pdf).

<sup>69</sup> ‘Appalling’ Anti-Terrorism Laws Draw Criticism, ABC News Online, 27 September 2005.

See also

Convention for the Suppression of the Financing of Terrorism and to “starve terrorists of assets and funds in order to reduce their capacity to operate.”<sup>70</sup>

The Financing of Terrorism Act amends Australia’s general Criminal Code by criminalizing “the provision or collection of funds to facilitate a terrorist act.” The Financing of Terrorism Act also provides, as McCulloch and colleagues explain, that “cash dealers and financing institutions to report suspected terrorist-related transactions,” “provide a penalty for using the assets of those allegedly involved in terrorist activities,” “streamline the process for disclosing financing transaction information to foreign countries,” and “allow for the freezing of assets of proscribed persons and entities.”<sup>71</sup>

The Australian financing of terrorism regime implicates charities in a number of ways – through potential penalties on individuals and on organizations, including proscription of organizations, for a range of acts. Charities and individuals in charities could in some cases be charged with various terrorist and terrorist financing offences. In specific terms, as a result of post-September 11 legislation, the Australian Criminal Code criminalizes committing a terrorist act (subsection 101.1), providing or receiving training connected to terrorist acts (101.2), possessing things connected with terrorist acts (101.4), collecting or making documents likely to facilitate terrorist acts (101.5), other acts done in preparation for or planning for terrorist acts (101.6), directing the activities of a terrorist organisation (102.2), membership in, recruiting for, providing or receiving training in connection with a terrorist organisation (102.3, 102.4, 102.5), getting funds to, from or for a terrorist organisation (102.6), providing support to a terrorist organisation (102.7), associating with a terrorist organisation (102.8), with separate additional offenses for financing terrorism or a terrorist (103.1, 103.2). Individuals connected to charitable organizations may also be subject to the control orders or preventative detention provided in subsections 104 and 105 of the Code.

---

<sup>70</sup> Jude McCulloch, Sharon Pickering, Rob McQueen, Joo-Cheong Tham and David Wright-Neville, Suppressing the Financing of Terrorism, 16 *Current Issues in Criminal Justice* 71-78 (2004). See also Jude McCulloch and Sharon Pickering, Suppressing the Financing of Terrorism: Proliferating State Crime, Eroding Censure and Extending Neo-colonialism, 45 *British Journal of Criminology* 470 (2005).

<sup>71</sup> McCulloch et al, id., also citing M Tan, Money Laundering and the Financing of Terrorism, 14(2) *Journal of Banking and Finance Law and Practice* 81-107 (2003).



Some of the few commentators on this legal regime raised challenging questions. McCulloch and colleagues, for example, suggest that “[i]ncreased regulation and surveillance of non-profit organisations and charities may undermine the ability of legitimate organisations to operate effectively in addition to curtailing their political independence. The flexibility of the definition of terrorism and the ease with which governments can deem organisations ‘terrorist’ for the purpose of freezing assets may result in some politically inconvenient or dissident charities and non-profit organisations being labeled terrorist organisations.”<sup>72</sup>

The workings of this legislation in practice have also raised concerns. Under the legislation discussed above and the *Charter of United Nations Act 1945* (Cth), for example, the Liberation Tigers of Tamil Eelam (LTTE) had been proscribed in Australia, making it a criminal offense to donate, provide funds or deal in the assets of the proscribed group, regardless of purpose, including humanitarian assistance. “This is of grave concern,” wrote one of Australia’s leading civil liberties organizations, Liberty Victoria, “especially given that the Australian Federal Police has acted upon this listing by raiding Tamil Co-ordinating Committee of Australia in November last year....The effect of these raids has been to generate fear amongst the Sri Lankan Tamil communities in Australia.”<sup>73</sup>

The Report of the Security Legislation Review Committee (SLRC), released in June 2006, picked up on these criticisms and expanded them. The SLRC specifically criticized portions of the anti-terrorism amendments to the Criminal Code that “appear to have a disproportionate effect on human rights and could be subject to administrative law challenge.”<sup>74</sup> The SLRC recommended that these provisions be repealed or changed. The problematic legal provisions include<sup>75</sup>:

1. Process for proscription. The SLRC called for revamping “the process for proscribing and organization as a terrorist organisation” under Criminal Code subsection 101.2, noting that

<sup>72</sup> McCulloch et al, supra note 70. On Australian constitutional issues with this legislation and its impact, see Joo-Cheong Tham, Possible Constitutional Objections to the Powers to Ban ‘Terrorist’ Organisations, 27 *University of New South Wales Law Journal* 482 (2004).

<sup>73</sup> Liberty Victoria submission on the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth), 10 December 2006.

<sup>74</sup> Report of the Security Legislation Review Committee (June 2006), p. 4, available at [www.ag.gov.au/www/agd/agd.nsf/Page/National\\_securityReviewsSecurity\\_Legislation\\_Review\\_Committee](http://www.ag.gov.au/www/agd/agd.nsf/Page/National_securityReviewsSecurity_Legislation_Review_Committee). For the detailed recommendations, see pp. 8-16.

<sup>75</sup> Separate citations are not provided for each section below; all these recommendations and the specific quotations are found at id., pp. 3-16. Individual citations available on request.

"no sufficient process is in place that would enable persons affected by such proscription to be informed in advance that the Attorney-General is considering whether to proscribe the organisation, and to answer the allegation that the organisation is a terrorist organisation. A consequence of proscription is that, on account of their connection with the organisation, persons become upon proscription liable to criminal prosecution. In that prosecution the defendant cannot deny that the proscribed organisation is a terrorist organisation or for that matter 'an organisation'. All members of the SLRC believe that a fairer and more transparent process should be devised for proscribing an organisation as a terrorist organisation."

The SLRC recommended that the proscription process be improved either by enhancing the protective and notice aspects of executive proscription, or by making proscription a judicial process with notice, service and a judicial hearing. The grounds for proscription were broadened in 2005 to include organizations that advocate the doing of a terrorist act.

2. Advocating terrorist acts. The SLRC noted that "advocating the doing of a terrorist act is one of the grounds for proscription of an organisation as a terrorist organisation," and called for the deletion of a portion of the broad definition of "advocates" in section 102.1(1A) in the Criminal Code that creates liability for "directly prais[ing] the doing of a terrorist act in circumstances where there is a risk that such praise might lead a person to engage in a terrorist act."<sup>76</sup> The SLRC called that provision "on its face, broad and potentially far-reaching." If its deletion were not possible, the SLRC stated that "the paragraph should be more tightly defined and changed to require that the risk be a substantial risk."

3. Association. The SLRC also directly criticized the offence of "associating with terrorist organizations" that was added to the Australian Criminal Code in 2004.

"On its face, this offence transgresses a fundamental human right – freedom of association – and interferes with ordinary family, religious and legal communication....

[S]ection 102.8 should be repealed. The interference with

---

<sup>76</sup> Here the SLRC is paraphrasing rather than directly citing section 102.1(1A).

human rights is disproportionate to anything that could be achieved by way of protection of the community if the section were enforced....[T]he most important feature of the section – making it an offence to provide support to a terrorist organization with the intention that the support assists the organisation to expand or to continue to exist – can be achieved by a new offence that does not rely on association between the person charged and anyone else.”

4. Strict liability. The SLRC called for the repeal or amendment of several Criminal Code subsections applying strict liability (punishment without proof of fault - a concept quite similar to absolute liability in Canada).

5. Definition of terrorist act. The SLRC recommended that the definition of “terrorist act” in the Criminal Code also be amended by “omitting all reference to ‘threat of action’.” Its place in the definition causes uncertainty and is unnecessary.” The SLRC recommended a separate offence for “threatening action” or “threat to commit a terrorist act” if that would be considered necessary.

The SLRC concluded that “the amendments ... recommended to the proscription, advocacy, association and strict liability elements of Part 5.3 of the Criminal Code would contribute to a reduction in fear and sense of alienation by at least some Muslim and Arab Australians. By doing so, there will be an enhancement, not a diminution, of anti-terrorism efforts.”

6. Training. The SLRC also recommended that the provision of the Criminal Code that criminalizes “training a terrorist organisation or receiving training from a terrorist organisation” be amended to “make it an element of the offence either that the training is connected with a terrorist act or that the training is such as could reasonably prepare the organisation, or the person receiving the training, to engage in, or assist with, a terrorist act,” and that the offence should not be a strict liability offence.

7. Funding to, from or for a terrorist organisation. The SLRC recommended that the current broad offence of “getting funds to, from or for a terrorist organisation” under subsection 102.6 should “not apply to the person’s receipt of funds from the organisation ... solely for the purpose of the provision of ... legal representation ... or assistance to the organisation for it to comply with ... law....”

8. Providing support to a terrorist organization. The SLRC recommended that the support offence “be amended to ensure that the word ‘support’ cannot be construed in any way to extend to the publication of views that appear to be favourable to a proscribed organization and its stated objective,” reflecting freedom of expression concerns about the breadth of the support proscription.

Contrasted with the warnings and limitations suggested by the Security Legislation Review Committee, the new Anti-Money Laundering and Counter-Terrorism Financing Act, adopted in 2006, will potentially increase the impact on the Australian charitable sector. The Act is intended to bring Australia into compliance with the Financial Action Task Force (FATF) standards.

The Act<sup>77</sup> primarily affects “financial and gambling sectors, bullion dealers and lawyers/accountants (but only to the extent that they provide financial services in direct competition with the financial sector – legal professional privilege will still apply) who provide designated services,” and will be expanded to include further coverage of “real estate agents, jewellers, lawyers and accountants.” The Act’s definition of “designated services” covers “a wide range of financial services including opening an account, accepting money on deposit, making a loan, issuing a bill of exchange, a promissory note or a letter of credit, issuing a debit or stored value card, issuing traveller’s cheques, sending and receiving electronic funds transfer instructions, making money or property available under a designated remittance arrangement, acquiring or disposing of a bill of exchange, promissory note or letter of credit, issuing or selling a security or derivative, accepting a contribution, roll-over or transfer in respect of a member of a superannuation fund and exchanging currency.”<sup>78</sup> It is thus possible that a charitable or other organization undertaking such services would fall within the purview of the Act, perhaps for accepting

---

<sup>77</sup> The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 is at [www.comlaw.gov.au/comlaw/legislation/act1.nsf/asmade/bytitle/AD9D7C024DC9E300CA257244001003BF?OpenDocument](http://www.comlaw.gov.au/comlaw/legislation/act1.nsf/asmade/bytitle/AD9D7C024DC9E300CA257244001003BF?OpenDocument); the Explanatory Memorandum is at [www.comlaw.gov.au/comlaw/legislation/bills1.nsf/bills/bytitle/666CB8390F7D8E10CA25721900788934?OpenDocument&VIEWCAT=attachment&COUNT=999&START=1](http://www.comlaw.gov.au/comlaw/legislation/bills1.nsf/bills/bytitle/666CB8390F7D8E10CA25721900788934?OpenDocument&VIEWCAT=attachment&COUNT=999&START=1).

<sup>78</sup> Explanatory Memorandum, p. 1.



a contribution, or sending EFT instructions, even if it is not a designated target of the legislation.

Thus, according to a close Australian observer of this sector and the legislation, “funds received from this [charitable and nonprofit] sector will be subject to the provisions of the [Act]. Obligations are generally imposed on ‘reporting entities’, that is, entities providing ‘designated services’ (s 5). ‘Designated services’ cover a range of financial services (... s 6, Table 1) hence, charitable and nonprofit organisations receiving designated services will be affected by the [Act] in the sense that ‘reporting entities’ when discharging their obligations under the regime will be collecting financial information regarding these organisations and, in some circumstances, forwarding them on to AUSTRAC (and from then on to security and police agencies).”<sup>79</sup>

Australian nonprofits and charities may also be “subject to special attention when ‘reporting entities’ seek to comply with their obligations under the [Australian] AML/CTF regime”<sup>80</sup> because the Act seeks to codify Australia’s commitments under the FATF standards, and a key focus of the FATF, through Special Recommendation VIII, has been with nonprofit organizations. The new Act also regulates what it terms “designated remittance arrangements,” which “is the [Act]’s synonym for alternative remittance systems like hawala.”<sup>81</sup> So such groups – which may be nonprofit or charitable organizations or have close links to them – will be affected by the Act’s requirements of such “designated remittance arrangements,” including reporting requirements as “reporting entities” under the Act (sec. 6) and registration requirements (part 6). One potential concern here is that the Act would be used for indirect and selective regulation of charities and perhaps those that provide services to them.

The Act was roundly criticized by industry, civil liberties, academic and other representatives during the mandatory comment period. At least one organization – Liberty Victoria, a leading civil liberties group, specifically raised the problem of impact on the charitable sector.

---

<sup>79</sup> Communication from Australian academic.

<sup>80</sup> Id.

<sup>81</sup> Id.

Liberty Victoria noted that because the underlying “financing of terrorism” offenses (discussed above, sec. 102.6 of the Criminal Code) are “very broad and capture conduct that go far beyond intentional funding of politically or religiously motivated violence,” including criminalizing donation of money to groups like Hamas “for the sole purpose of assisting its humanitarian activities,” and because “all but one of the listed ‘terrorist organisations’ under the Criminal Code are self-identified Muslim groups, the Criminal Code ‘terrorist organisation’ provisions have resulted in a tangible sense of fear and uncertainty amongst Muslim Australians especially in relation to charity giving.”<sup>82</sup>

Liberty Victoria cites a member of the Islamic Council of Victoria on the effect of this legislation, and its potential compounding in the new Act: “This level of uncertainty in an offence this serious is deeply worrying. And for Australian Muslims, doubly so. Because charity is one of the five pillars on which Islamic practice is built, Muslims tend to be a charitable people. That is especially true at certain times of the Islamic year when charity is religiously mandated. Countless fund-raising efforts followed the tsunami and the Pakistan earthquake, and even in the normal course of events, Muslim charities regularly provide relief to parts of the Muslim world many other charities forget.”<sup>83</sup>

Liberty Victoria disputes the necessity of such provisions—as well as the idea that they faithfully reflect Australia’s obligations under the International Convention for the Suppression of the Financing of Terrorism and the Financial Action Task Force’s Special Recommendations on Terrorist Financing. In reality, writes Liberty Victoria, “both these documents, while calling for the criminalisation of the financing of terrorism, define financing of terrorism in a narrower manner than sections 20-1 of the *Charter of United Nations Act 1945* (Cth) and section 102.6 of the *Criminal Code*, by emphasising the need for an intention or knowledge that funds will be used to carry out terrorism.” “[B]y not requiring that there be intention or knowledge that funds be used to facilitate acts of violence, [the Australian legislation] is at odds” with these international standards.<sup>84</sup>

---

<sup>82</sup> Liberty Victoria submission on the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth), 10 December 2006.

<sup>83</sup> Liberty Victoria, id., citing Waleed Aly, *Reckless Terror Law Threatens to Make Charity End at Home*, *The Age* (Melbourne), 29 November 2005, 15.

<sup>84</sup> Liberty Victoria, id.

For Liberty Victoria, the solution is reasonably clear: the offenses in a separate section of the Australian Criminal Code, Division 103, “at least require that the funds have some connection with the engagement of a ‘terrorist act.’ It is, therefore, recommended that ‘financing of terrorism’ under the [new Act] be restricted to conduct that amount to an offence under Division 103 of the Criminal Code.”<sup>85</sup> That suggestion was not taken by the drafters.

Based on current information the enhanced Australian counter-terrorism statutory stream has not yet been used to proscribe charities on terrorism grounds or in other ways against charities. While new legislation may potentially have more effects on the charitable sector, the broad existing legislation does not appear to have been used against the charitable sector, and its effectiveness in halting any financial flows to terrorist organizations using charities and stopping terrorism might legitimately be questioned.

## General Conclusions

A number of common areas and lessons arise in the exploration of charities and terrorist finance in the United Kingdom, the United States, and Australia.

1. Statutes and regulation barring various forms of charitable assistance to or use by terrorists were generally in place before September 11. They were rapidly broadened in the ensuing several years, and have since been further broadened. In several countries still further broadening measures are underway.

2. Opposition from the charitable sector has been episodic at best, and most clearly focused in the United States, where the government’s voluntary guidelines on overseas giving have sparked discontent, particularly in the philanthropic sector. Charities and philanthropic organizations tend to become exercised by broadening government regulation in this area only when they are directly affected, as by the U.S. Treasury’s guidelines on overseas funding. The British approach, at which the Charity Commission’s regulatory role has thus far remained at the center of investigatory and enforcement activities, appears to have sparked less opposition from the voluntary sector.

---

<sup>85</sup> Liberty Victoria, id

3. Certain key issues appear to arise in each country. They include:

- The process, scope, intentionality requirement and reviewability of proscription decision making;
- The availability and fairness of a de-proscription process;
- The breadth of terrorist “support” or “material support” or “assistance” or “training” or financing offenses, including the frequent lack of a *mens rea* requirement and the breadth of the offense;’
- The dangers to associational freedom potentially posed by the broad legislation already enacted or proposed;
- The difficulty in preserving a central role for nonpolitical and nonpartisan charity regulators, where they exist; and other issues.

4. A key difference among these jurisdictions that may be of interest to the Commission is typified by the British and American cases. The British regulatory approach, with the Charity Commission at its center, focuses inquiries into suspicious cases, with a range of potential solutions that can include strengthened procedures, replacement of trustees and on up to closing and proscription of the charity. The American approach has been centered on prosecution for “material support” and other criminal charges, more recently supplemented by “voluntary guidelines” intended to promote compliance, particularly in the philanthropic sector. In my view the British approach may have worked more effectively in the years since 2001. The British case studies discussed above demonstrate that the Charities Commission employs a broad range of investigative and regulatory responses to concerns that charities have links with terrorism. Not all of the regulatory responses are punitive and can include requiring improved record-keeping and other measures that may make it easier to detect links with terrorists in the future. It should be noted, however, that the regulation of charities in Britain is centred in one level of government whereas the United States, Australia and Canada are all federations in which regulatory jurisdiction over charities are divided between different levels of government.



5. Self-regulation emerges with mixed success in these jurisdictions. In the United States, the self-regulatory approach of the Treasury's voluntary guidelines on overseas giving sparked opposition. Some charities attempted to comply with these voluntary guidelines through additional vetting procedures while some attempted to shift risk downstream to grantees through revised and strengthened grant letters. In Britain the sophistication and nuance of the Charity Commission and its role has perhaps reduced the need for a self-regulatory approach as the Commission has helped to educate the charitable sector as well as adopting a range of investigatory and enforcement measures.

Mark Sidel is Professor of Law, Faculty Scholar, and Lauridsen Family Fellow at the University of Iowa and a research scholar at the University's Obermann Center for Advanced Studies. He has written extensively about the impact of anti-terrorism law and policy on the nonprofit sector, philanthropy and civil society and was awarded the 2008 Civil Liberties Prize by the International Center for Not-for-Profit Law (ICNL) and the Catholic Organisation for Relief and Development (Cordaid) for his work on charities and counter-terrorism in the United States and the United Kingdom.

Sidel has served as Visiting Professor of Law at Harvard Law School (1998, 2005-06), Melbourne Law School (2005, 2008), University of Victoria (2007), and the Institut d'Etudes Politiques (Sciences Po, 2004), and as W.G. Hart Lecturer in Law at the School of Oriental and African Studies (SOAS) (2003).

Sidel has published *More Secure, Less Free? Anti-Terrorism Policy and Civil Liberties after September 11* (University of Michigan Press, 2004, revised and updated ed. 2007). His book on counter-terrorism and the nonprofit and philanthropic sector, *The Regulation of the Voluntary Sector: Freedom and Security in an Age of Uncertainty*, will be published by Routledge in 2009. Sidel recently convened a major conference at the University of Iowa on the impact of counter-terrorism law and policy on the voluntary sector in comparative perspective which brought together academic and policy specialists to discuss Canada, China, the European Union, Japan, Kenya, Korea, the Netherlands, Nigeria, Russia, Sri Lanka, the U.K., the U.S. and other areas.

Sidel currently serves as president-elect of the International Society for Third Sector Research (ISTR, president 2009-11), and chair-elect of the Nonprofit and Philanthropic Law Section of the American Association of Law Schools (AALS, chair 2009-10). He also works on comparative law in Asia and has published extensively in this area as well; his work includes *Law and Society in Vietnam* (Cambridge University Press, 2008), *Philanthropy and Law in South Asia* (ed. with Zaman, 2004 and updated volume 2007), and *Cinema, Law, and the State in Asia* (ed. with Creekmur, Palgrave Macmillan, 2007).

## **Charities and Terrorist Financing: A Review of Canada's Legal Framework**

**David G. Duff<sup>1</sup>\***

---

<sup>1</sup> Associate Professor, Faculty of Law, University of Toronto. Opinions expressed are those of the author and do not necessarily represent those of the Commissioner.





## Introduction

A decade after the bombing of Air India Flight 182 in June 1985, many Canadians were shocked to learn that the Babbar Khalsa Society – a militant organization dedicated to the establishment of an independent state in northern India, members of which are believed to have planned the Air India bombing – had been granted charitable status in Canada.<sup>1</sup> Although the organization's charitable status was revoked in 1996,<sup>2</sup> reports also suggested that funds collected to support Sikh temples in Canada may have been diverted to support Sikh militancy in India.<sup>3</sup> Concerns have also been raised about the role of other charitable organizations in terrorist financing – for example the Benevolence International Fund, an organization with links to al-Qaeda that was designated as a financier of terrorism by the U.S. Treasury Department in November 2002.<sup>4</sup>

In the months after the terrorist attacks of September 11, 2001, the Canadian government moved quickly to introduce various measures to constrain terrorist financing: adding several offences to the *Criminal Code*,<sup>5</sup> renaming and amending the *Proceeds of Crime (Money Laundering) Act* to address terrorist financing as well as money laundering,<sup>6</sup> and expanding the role of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) to combat terrorist financing.<sup>7</sup> In addition to these

<sup>1</sup> See the question addressed to the Minister of National Revenue by Val Meredith, Reform Party Member of Parliament for Surry-White Rock-South Langley, B.C. in *Hansard* (4 May 1995) at 12192-93. Charitable status was apparently granted in 1993. See Peter Hadzipetros, "Sikh Militancy," *CBC News Online* (27 August 2003), available at <http://www.cbc.ca/news/background/airindia.sikh.html>.

<sup>2</sup> *Ibid.*

<sup>3</sup> See, e.g., Ken MacQueen, "Air India Arrests" *Maclean's Magazine* (13 November 2000). According to this story: "When moderates finally took over control of Surrey's Guru Nanak temple in 1996, president Balwant Singh Gill says they found virtually no financial records for the past 10 years, leading to unproven speculation that the institution, with its 31,000 voting members, had inadvertently financed the fight for Khalistan. The temple was rundown and heavily mortgaged – where a decade of donations went, Gill can only guess. 'I can say one thing,' he says. 'The first year we took over this temple, in 1996, we paid out all the mortgage, \$848,000 in one year. And we did some construction work. In the 10 years before, nothing had been done to the temple: no construction, no repairs, no renovation.'"

<sup>4</sup> United States Department of Treasury, "Treasury Designates Benevolence International Foundation and Related Entities as Financiers of Terrorism" Press Release PO-3632 (19 November 2002), available at <http://www.treasury.gov/press/releases/po3632.htm>.

<sup>5</sup> R.S.C. 1985, c. C-46, Part II.1, ss. 83.01-83.27 [as amended]. For a summary of these provisions, see Anita Indira Anand, "An Assessment of the Legal Regime Governing the Financing of Terrorist Activities" Research Paper Prepared for Commission of Inquiry into the Investigation of the Bombing of Air India (2007) at 5-6. See also Kevin Davis, "Cutting off the Flow of Funds to Terrorists: Whose Funds? Which Funds? Who Decides?" in Ronald J. Daniels, Patrick Macklem and Kent Roach, eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*, (Toronto: University of Toronto Press, 2001) at 299-319.

<sup>6</sup> *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17 [as amended]. For a summary of these provisions, see Anand, *supra* note 1 at 8-11.

<sup>7</sup> See Department of Finance New Release, "FINTRAC Receives Increased Funding to Combat Terrorist Financing" (October 25, 2001), available at <http://www.fn.gc.ca/news01/01-094e.html>. Reference, (1 May 2006), paragraph (b)(iv).

measures, the federal government also enacted the *Charities Registration (Security Information) Act* (CRSIA),<sup>8</sup> providing for the denial or revocation of an organization's charitable status where there are reasonable grounds to believe that its resources are used to support terrorism.<sup>9</sup> More recently, the federal government introduced further measures to combat terrorist financing,<sup>10</sup> including amendments to the federal *Income Tax Act* (ITA)<sup>11</sup> that authorize the Canada Revenue Agency (CRA) to disclose specific categories of information about charitable organizations to the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP) and FINTRAC.

This report examines the legal framework governing charities in Canada in order to assist the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (Air India Inquiry) in its mandate to determine, among other things, "whether Canada's existing legal framework provides adequate constraints on terrorist financing" through "the use or misuse of funds from charitable organizations."<sup>12</sup> Part I reviews the constitutional framework governing the establishment and regulation of charities in Canada, considering the respective powers of the federal and provincial governments and the effect of this constitutional division of powers on the regulation of charities in Canada. Part II outlines the legal and administrative framework governing registered charities under the ITA and the CRSIA, explaining key legal rules and administrative practices affecting their status and operations, as well as the supervisory and regulatory role performed by the CRA. Part III examines the collection and sharing of information on charitable organizations for the purpose of administering ITA and CRSIA rules regarding charitable status as well as other measures to prevent terrorist financing. Part IV evaluates Canada's existing legal framework for constraining terrorist financing through charitable organizations, reviewing the adequacy of this framework in light of limits on federal jurisdiction over charities and the recent introduction of more flexible compliance-based approaches to charities regulation. Part V concludes.

---

<sup>8</sup> S.C. 2001, c. 41, s. 113.

<sup>9</sup> For a discussion of this legislation (on which part of this report is based), see David G. Duff, "Charitable Status and Terrorist Financing: Rethinking the Proposed *Charities Registration (Security Information) Act*" in Daniels, et. al., *supra* note 5 at 321-37.

<sup>10</sup> *An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the Income Tax Act and to make a consequential amendment to another Act*, S.C. 2006, c. 12.

<sup>11</sup> R.S.C. 1985, c. 1 (5<sup>th</sup> Supp.) [as amended].

<sup>12</sup> Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, Terms of

## I. Constitutional Framework Governing Charities in Canada

According to subsection 92(7) of the *Constitution Act, 1867*,<sup>13</sup> provincial legislatures in Canada are granted exclusive authority to make laws in relation to: "The Establishment, Maintenance, and Management of ... Charities, and Eleemosynary Institutions in and for the Province." In addition, provinces have exclusive jurisdiction over "Property and Civil Rights in the Province"<sup>14</sup> – allowing them to regulate the transfer and use of property for charitable purposes. Federal jurisdiction over charities, on the other hand, is limited to the incidental powers that the Parliament of Canada derives from its taxation power.<sup>15</sup> To the extent that the ITA confers special tax benefits on charities and their contributors, supervision and regulation of charities in order to ensure that they satisfy the terms on which these benefits are conferred constitutes a legitimate exercise of this federal power. While provincial governments have broad powers to regulate charities and charitable property, therefore, federal jurisdiction to supervise and regulate charities is limited to conferral of fiscal benefits under the ITA.

Notwithstanding their constitutional authority to regulate charities and charitable donations, most provinces have either chosen not to exercise this jurisdiction,<sup>16</sup> or have done so only sparingly.<sup>17</sup> Although a few provinces have enacted legislation regarding charitable fundraising,<sup>18</sup> and provincial Attorneys-General have the right and duty to supervise and assist charities under their *parens patriae* jurisdiction as representatives of the Crown,<sup>19</sup> only Ontario has enacted specific legislation regulating the operation of charitable organizations and the use of charitable property in the province.<sup>20</sup> As a result, as Patrick Monahan and Elie Roth observe

<sup>13</sup> U.K., 30 & 31 Victoria, c.3.

<sup>14</sup> *Ibid.*, subsection 92(13).

<sup>15</sup> *Ibid.*, subsection 91(3), granting the Parliament of Canada authority to make laws for: "The raising of Money by any Mode or System of Taxation."

<sup>16</sup> Patrick J. Monahan with Elie S. Roth, *Federal Regulation of Charities: A Critical Assessment of Recent Proposals for Legislative and Regulatory Reform*, (Toronto: York University, 2000) at

<sup>17</sup> Arthur B.C. Drache, "The English Charity Commission Concept in the Canadian Context", 1997, 14 *The Philanthropist* 8.

<sup>18</sup> *Charitable Fund-Raising Act*, R.S.A. 2000, c. C.9 (Alberta); *The Charities Endorsement Act*, R.S.M. c. C60 (Manitoba); and *The Charitable Fund-Raising Business Act*, S.S. 2002, c. C-6.2 (Saskatchewan).

<sup>19</sup> Kenneth R. Goodman, "Standing on Guard for Thee: The Role of the Office of the Public Guardian and Trustee" (2002), 17 *The Philanthropist* 4.

<sup>20</sup> *Charities Accounting Act*, R.S.O. 1990, c. C.10. This legislation was first enacted in 1915, and was based on English law and legal practice prevailing at the time. For a general overview of this legislation, see Goodman, *supra* note 19. For a more detailed and critical examination of this regulatory regime, with specific recommendations for reform, see Ontario Law Reform Commission (OLRC), *Report on the Law of Charities*, Vol. 2 (Toronto: Queen's Printer, 1996), chapter 17.



in their study on *Federal Regulation of Charities*, “the federal government, though the scheme of regulation enacted for charities pursuant to the *Income Tax Act* (“ITA”), has *de facto* assumed the dominant regulatory role in this sector.”<sup>21</sup>

Since federal jurisdiction over charities extends only to the conferral of fiscal benefits under the ITA, however, this regulatory role is much more limited than might be exercised under provincial jurisdiction. In Ontario, for example, the *Charities Accounting Act* grants the Public Guardian and Trustee and the Superior Court of Justice broad supervisory powers over charities operating in Ontario, including the power to remove trustees or executors and appoint other persons to act in their place.<sup>22</sup> Such extensive supervisory powers are unavailable at the federal level, absent provincial delegation to a federal body or the establishment of a joint federal-provincial agency.<sup>23</sup>

Moreover, because federal jurisdiction over charities is incidental to its taxing power, federal regulatory efforts in this area have tended to emphasize monitoring and investigation in order to assess eligibility for tax benefits, rather than advice and support in order to assist charities to carry out their activities in a manner consistent with their legal obligations and charitable purposes.<sup>24</sup> While recent federal initiatives have placed increased emphasis on advice and support, for example through a Charities Partnership and Outreach Program that funds education and training programs for registered charities,<sup>25</sup> these initiatives focus mainly on compliance with the ITA.<sup>26</sup> Together with the recent introduction of

<sup>21</sup> Monahan with Roth, *supra* note 16 at 7. See also Drache, *supra* note 17 at 10, explaining that “because complying with the tax rules is crucial to virtually all charities in Canada, *de facto* Revenue Canada has become the most important overseer.”

<sup>22</sup> *Charities Accounting Act*, *supra* note 20, s. 4(g). According to the statute, the Superior Court may make an order to this effect, upon application by the Public Guardian and Trustee, if the charity “refuses or neglects to comply” with obligations to report information or submit its accounts to be examined by the Court, is determined to have “misapplied or misappropriated any property or fund” coming into its hands, has made “any improper or unauthorized investment” of charitable funds, or “is not applying any property, fund or money in the manner directed by the will or instrument” establishing a charitable purpose trust or charitable corporation. The statute also allows persons who allege a breach of a trust created for a charitable purpose to apply to the Superior Court which may “make such order as it considers just for carrying out of the trust under the law.” *Ibid.*, s. 10(1).

<sup>23</sup> Monahan with Roth, *supra* note 16 at 97.

<sup>24</sup> Drache, *supra* note 17 at 10. See also OLRC, *supra* note 20, Vol. 1, at 262.

<sup>25</sup> See, e.g., Canada Revenue Agency, “Government delivers innovative \$2 million program for charities and non-profit organizations,” News Release (31 October 2006), available at <http://www.cra-arc.gc.ca/newsroom/releases/2006/oct/nr061031b-e.html>.

<sup>26</sup> See, e.g., Canada Revenue Agency, “Charities Partnership and Outreach Program,” available at <http://www.cra-arc.gc.ca/tax/charities/funding/menu-e.html>, explaining that the “overall objective” of the Charities Partnership and Outreach Program is “to increase compliance by the charitable sector with relevant parts of the *Income Tax Act*.”



various “intermediate” penalties and sanctions in addition to the ultimate punishment of revocation,<sup>27</sup> however, these initiatives signal a major shift in the federal government’s regulatory approach to the charitable sector from a traditional emphasis on the enforcement of inflexible rules to a more responsive approach aimed at encouraging compliance.<sup>28</sup>

## II. Legal and Administrative Framework Governing Registered Charities

As explained in the previous Part of this report, the sole reason for federal supervision and regulation of charities is to ensure that they satisfy the terms on which fiscal benefits are conferred under the ITA. The following sections explain the legal framework governing registered charities under the ITA and the CRSIA, reviewing the fiscal benefits that the ITA confers on charities and their contributors, the statutory and judicial tests that an organization must satisfy in order to register for charitable status under the ITA, the legal and administrative requirements that a registered charity must fulfill in order to maintain this status, the penalties and sanctions that the ITA imposes on charities that fail to comply with these requirements, and the additional legal implications of the CRSIA.

### 1. Fiscal Benefits

Charitable status confers two fiscal benefits under the ITA. First, like many other organizations, such as non-profit organizations, registered charities are exempt from tax on their income.<sup>29</sup> Second, qualifying gifts to registered charities are eligible for further tax benefits in the form of a

---

<sup>27</sup> ITA, ss. 181.1 and 181.2, applicable to taxation years after March 22, 2004. These “intermediate” measures are reviewed in Part II of this report.

<sup>28</sup> See, e.g., Susan D. Phillips, “Governance, Regulation and the Third Sector: Responsive Regulation and Regulatory Responses” Paper Presented to the Annual Meeting of the Canadian Political Science Association, London, Ontario (2 June 2005). On the theory of responsive regulation more generally, see John Braithwaite, *Restorative Justice and Responsive Regulation*, (Oxford: Oxford University Press, 2002), chapter 2.

<sup>29</sup> ITA, s. 149(1)(f).

non-refundable credit for individual donors,<sup>30</sup> a deduction for corporate donors,<sup>31</sup> and an exemption from capital gains tax on gifts of publicly-traded securities and ecologically sensitive land.<sup>32</sup> While these tax benefits for qualifying gifts are not available for donations to non-profit organizations, they are available for qualifying gifts to other entities such as registered Canadian amateur athletic associations, low-cost housing corporations, Canadian municipalities, the United Nations, and Her Majesty in right of Canada or a province.<sup>33</sup> Collectively, the ITA defines these entities as “qualified donees.”<sup>34</sup>

Although various rationales may be advanced in favour of these tax provisions,<sup>35</sup> they are generally viewed as incentives or “tax expenditures” that are designed to provide an indirect subsidy to registered charities and other qualified donees by encouraging individuals and corporations to make donations to these entities. A subsidy for these entities is generally justified on the grounds that they provide public benefits that would otherwise be undersupplied, and perform quasi-governmental functions that would otherwise have to be financed directly from tax revenues.<sup>36</sup> The indirect form of this subsidy in the form of a tax incentive is often favoured as a more pluralistic method of subsidizing these activities than direct subsidies – allowing donors to select the organizations and purposes to which they wish to direct public subsidies without having to obtain the agreement of a political majority.<sup>37</sup> The annual cost of these

<sup>30</sup> ITA, s. 118.1. At the federal level, this credit is computed at the lowest marginal rate of tax for the first \$200 of total gifts claimed in the taxation year and the highest marginal rate for amounts exceeding \$200. For the 2007 taxation year, the federal rate structure implies a credit of 15.25 percent on the first \$200 claimed each year and 29 percent on amounts over \$200. Most provinces and territories adopt a similar two-tiered rate structure for their charitable contributions tax credits, which generally range from 4 to 11 percent on the first \$200 and from 11.5 to 18.02 percent on amounts above this threshold. In Quebec, the credit is computed at a rate of 20% on the first \$2,000 claimed in the year, and 24% on amounts exceeding \$2,000.

<sup>31</sup> ITA, s. 110.1.

<sup>32</sup> ITA, ss. 38(a.1) and (a.2).

<sup>33</sup> See ss. 38(a.1) and (a.2), s. 110.1(1)(a), and the definition of “total charitable gifts” in s. 118.1(1).

<sup>34</sup> ITA, s. 149.1(1).

<sup>35</sup> For a review and critical evaluation of alternative rationales for the tax recognition of charitable contributions, see David G. Duff, “Tax Treatment of Charitable Contributions: Theory, Practice, and Reform” (2004), 43 *Osgoode Hall L.J.* 47 at 50-70.

<sup>36</sup> See, e.g., Lester M. Salamon, “Partners in Public Service: The Scope and Theory of Government-Non-profit Relations,” in Walter Powell, ed., *The Non-profit Sector: A Research Handbook* (New Haven, Conn.: Yale University Press, 1987) 99; and Rick Krever, “Tax Deductions for Charitable Donations: A Tax Expenditure Analysis” in Richard Krever and Gretchen Kewley, eds., *Charities and Philanthropic Institutions: Reforming the Tax Subsidy and Regulatory Regimes*, (Melbourne: Australian Tax Research Foundation, 1991) 1 at 8-13.

<sup>37</sup> See, e.g., Krever, “Tax Deductions and Charitable Donations,” *supra* note 36 at 11-13; and David G. Duff, “Charitable Contributions and the Personal Income Tax: Evaluating the Canadian Credit” in Jim Phillips, Bruce Chapman, and David Stevens, eds., *Between State and Market: Essays on Charities Law and Policy in Canada*, (Montreal and Kingston: McGill-Queen’s University Press, 2001) 407 at 433-36.

incentives in terms of foregone revenues was estimated at over \$2 billion in 2003 and is projected to rise to almost \$2.5 billion in 2008.<sup>38</sup>

## 2. Obtaining Registered Charitable Status

Although the federal income tax has provided fiscal benefits of one sort of another to charities since it was first enacted in 1917,<sup>39</sup> it was not until 1967 that the federal government established a registration system for Canadian charities, requiring all organizations issuing charitable receipts for qualifying gifts to apply for and maintain registered status under the ITA.<sup>40</sup> Since then, federal revenue authorities have exercised primary supervisory and regulatory authority over Canadian charities through their authority to grant or revoke the organization's status as a registered charity.<sup>41</sup> As of December 2005, over 82,000 charities were registered with the CRA,<sup>42</sup> representing roughly half of all nonprofit and voluntary organizations in Canada.<sup>43</sup> Most of these organizations have annual revenues less than \$100,000,<sup>44</sup> and many rely on unpaid volunteers.<sup>45</sup>

In order to obtain charitable status under this registration system, an organization must satisfy statutory requirements under the ITA, judicial tests governing the meaning of a "charitable" purpose or activity, and administrative requirements adopted by the CRA. Beginning with

<sup>38</sup> Department of Finance, *Tax Expenditures and Evaluations*, (Ottawa: Her Majesty the Queen in Right of Canada, 2006) at 17 and 26

<sup>39</sup> *The Income War Tax Act, 1917*, 7-8 Geo 5, c. 28 (Can.), ss. 3(1)(c) (allowing a deduction for "amounts paid by the taxpayer during the year to the Patriotic and Red Cross Funds, and other patriotic and war funds approved by the Minister") and 5(d) (exempting the income of "religious, charitable, agricultural and educational institutions"). Although the deduction for patriotic and war funds was repealed in 1920, a more general deduction for charitable donations was subsequently enacted in 1930: *An Act to amend the Income War Tax Act*, S.C. 1930, c. 24, s. 3, enacting s. 5(1)(j) of the *Income War Tax Act*, R.S.C. 1927, c. 97. This deduction remained until 1988, when it was replaced with a non-refundable credit for individuals under section 118.1 of the ITA. For a detailed history of federal supervision of charities under the ITA, see OLRC, *supra* note 20, Vol. 1, at 249-86.

<sup>40</sup> *An Act to amend the Income Tax Act*, S.C. 1966-67, c. 47, ss. 3 and 15, amending *Income Tax Act*, R.S.C. 1952, c. 148, ss. 27 and 125.

<sup>41</sup> Although a decision to reject or revoke charitable status may be appealed to the Federal Court of Appeal under s. 172(3) of the ITA, the number of such appeals is extremely small. See *infra* note 69 and accompanying text.

<sup>42</sup> Canada Revenue Agency, *Registered Charities Newsletter*, No. 27 (Fall 2006) at 2, available at <http://www.cra-arc.gc.ca/E/pub/tg/charitiesnews-27/README.html>.

<sup>43</sup> Statistics Canada, *Cornerstones of Community: Highlights of the National Survey of Nonprofit and Voluntary Organizations, 2003 revised*, (Ottawa: Minister of Industry, 2005), available at [http://www.nonprofitscan.ca/pdf/NSNVO\\_Report\\_English.pdf](http://www.nonprofitscan.ca/pdf/NSNVO_Report_English.pdf) at 8.

<sup>44</sup> *Ibid.* at 34, reporting that 41.5% of nonprofit and voluntary organizations in Canada in 2003 had annual revenues less than \$30,000 and 21.3% had annual revenues of \$30,000 to \$99,000.

<sup>45</sup> *Ibid.* at 36, Table 3.8, reporting that 54% of nonprofit and voluntary organizations in Canada in 2003 had no paid staff.

statutory requirements under the ITA, subsection 248(1) defines a “registered charity” as a charitable organization, private foundation or public foundation (or division thereof) that is resident in Canada and was either created or established in Canada, provided that it has “applied to the Minister in prescribed form for registration, and is at that time registered as a charitable organization, private foundation or public foundation”. For the purpose of this definition, Form T2050 is prescribed as the form through which an application for charitable status must be made, and subsection 149.1(6.3) stipulates that the Minister of National Revenue may, by notice sent by registered mail to the registered charity, designate the charity to be a charitable organization, private foundation or public foundation, whereupon “the charity shall be deemed to be registered as a charitable organization, private foundation or public foundation, as the case may be, for taxation years commencing after the day of mailing of the notice unless and until it is otherwise designated ... or its registration is revoked ....”

The meanings of the terms charitable organization, private foundation and public foundation appear in section 149.1 of the ITA, which contains further statutory rules governing the acquisition and maintenance of charitable status. According to subsection 149.1(1), a charitable organization means an organization, whether or not incorporated,

- (a) all the resources of which are devoted to charitable activities carried on by the organization itself,
- (b) no part of the income of which is payable to, or is otherwise available for, the personal benefit of any proprietor, member, shareholder, trustee or settlor thereof, [and]
- (c) more than 50% of the directors, trustees, officers or like officials of which deal with each other and with each of the other directors, trustees, officers or officials at arm’s length ...

while a “charitable foundation” means

a corporation or trust that is constituted and operated exclusively for charitable purposes, no part of the income of which is payable to, or otherwise available for, the personal benefit of any proprietor, member, shareholder, trustee or settlor thereof, and that is not a charitable organization.

Where most of the officials of a charitable foundation deal with each other at arm’s length and no more than 50% of the foundation’s capital



was contributed by a single person or by members of a group who do not deal with each other at arm's length, the ITA classifies the foundation as a "public foundation"; otherwise, the charitable foundation is classified as a "private foundation".<sup>46</sup>

While the distinction between a public and private foundation turns on the extent to which it is controlled by a single person or related group, the distinction between a charitable organization and a charitable foundation generally turns on the manner in which they engage in charitable pursuits. As a general rule, charitable organizations must devote their resources to "charitable activities" that they themselves carry on.<sup>47</sup> As an administrative practice, moreover, the CRA recognizes as charitable activities carried on by a registered charity any charitable activity that is carried on outside Canada through an intermediary such as an agent, a contractor or other body.<sup>48</sup> In contrast, charitable foundations are merely required to operate for "charitable purposes" – a term which the ITA specifically defines to include "the disbursement of funds to qualified donees".<sup>49</sup> In general, therefore, charitable organizations engage in charitable activities themselves or through intermediaries, while charitable foundations operate for charitable purposes by disbursing funds to charitable organizations and other qualified donees.

Notwithstanding these differences between charitable organizations and charitable foundations, the ITA requires both types of registered

<sup>46</sup> For foundations registered before February 16, 1984, the distinction between a public and private foundation depends on a threshold of 75% of contributions of capital by a single person or group of persons not dealing with each other at arm's length, rather than 50%.

<sup>47</sup> Subsection 149.1(6) relaxes this requirement by considering a charitable organization to be devoting its resources to charitable activities carried on by it where it carries on a related business, disburses not more than 50% of its income to qualified donees, or disburses income to a registered charity with which it is "associated". According to s. 149.1(7) of the ITA, the Minister may on application designate a registered charity as a charity associated with one or more registered charities where "the Minister is satisfied that the charitable aim or activity of each of the registered charities is substantially the same ...."

<sup>48</sup> Canada Revenue Agency, RC4106 "Registered Charities Operating Outside Canada" available online at <http://www.cra-arc.gc.ca/E/pub/tg/rc4106/README.html>. According to this document, "[t]hese arrangements can be an acceptable devotion of the charity's resources to its 'own activities' providing: the charity has obtained reasonable assurance before entering into agreements with individuals or other organizations that they are able to deliver the services required by the charity (by virtue of their reputation, expertise, years of experience, etc.); all expenditures will further the Canadian charity's formal purposes and constitute charitable activities that the Canadian charity carries on itself; an adequate agreement is in place [as suggested in the document]; the charity provided periodic, specific instructions to individuals of organizations as and when appropriate; the charity regularly monitors the progress of the project or program and can provide satisfactory evidence of this ...; and, where appropriate, the charity makes periodic payments on the basis of this monitoring (as opposed to a single lump sum payment) and maintains the right to discontinue payments at any time if not satisfied."

<sup>49</sup> See the definition of "charitable purposes" in s. 149.1(1) of the ITA.

charity to be “exclusively charitable” – devoting “all” of their “resources” to charitable activities in the case of charitable organizations, and operating “exclusively” for charitable purposes in the case of charitable foundations. Where a charitable foundation or organization devotes “substantially all of its resources” to charitable purposes (in the case of a charitable foundation) or charitable activities carried on by it (in the case of a charitable organization), however, subsections 149.1(6.1) and (6.2) permit the charity to devote part of its resources to “political activities” provided that they are “ancillary and incidental” to the foundation’s purposes or the organization’s activities and “do not include the direct or indirect support of, or opposition to, any political party or candidate for public office”. More generally, judicial decisions have held that the pursuit of purposes that are not themselves charitable, but “incidental to” or “a means to the fulfillment of” other charitable purposes” will not deprive an organization or foundation of charitable status.<sup>50</sup>

Since the ITA does not, aside from these provisions, define the terms “charitable activities” and “charitable purposes”, Canadian courts have generally sought guidance in the common law of trusts, which admits charitable purpose trusts as an exception to the general rule that a purpose trust is invalid. Although the definition of a charitable organization mentions charitable activities, not purposes, the Supreme Court of Canada has downplayed the distinction, stating that “it is really the purpose in furtherance of which an activity is carried out, and not the character of the activity, that determines whether or not it is of a charitable nature.”<sup>51</sup> Where an organization is established for a charitable purpose, however, the Court has also emphasized that it is necessary to consider the activities carried on by the organization in order to ensure that they are “in furtherance of” the charitable purpose.<sup>52</sup>

---

<sup>50</sup> *British Launderers’ Research Association v. Borough of Hendon Rating Authority*, [1949] 1 K.B. 462 (C.A.), cited with approval by the Supreme Court of Canada in *Guaranty Trust Co. of Canada v. M.N.R.*, [1967] S.C.R. 113 at 143 (hereafter *Guaranty Trust*).

<sup>51</sup> *Vancouver Society of Immigrant and Visible Minority Women v. M.N.R.*, [1999] 1 S.C.R. 10 at para. 152.

<sup>52</sup> *Ibid.* at para.194.

The traditional starting point for judicial interpretations of charitable purposes is Lord Macnaghton's statement in *Commissioners for Special Purposes of the Income Tax v. Pemsel*,<sup>53</sup> that:

"Charity" in its legal sense comprises four principal divisions: trusts for the relief of poverty; trusts for the advancement of education; trusts for the advancement of religion; and trusts for other purposes beneficial to the community, not falling under any of the preceding heads.

Superimposed on these categories, however, is a further requirement that the purpose of the trust must be "[f]or the benefit of the community or of an appreciably important class of the community."<sup>54</sup> On the basis that judges cannot and/or should not determine whether a proposed change in the law is for the public benefit,<sup>55</sup> moreover, the courts and revenue authorities have traditionally denied charitable status where the activities or purposes of the organization or foundation advocate social change or promote a particular ideological outlook.<sup>56</sup>

Consistent with these statutory requirements and judicial tests, registration as a charitable organization or foundation by the CRA depends on a determination that the applicant is "constituted and operated exclusively for charitable purposes" under one of the four *Pemsel* categories,<sup>57</sup> that it satisfies the public benefit test,<sup>58</sup> and that

<sup>53</sup> [1891] A.C. 531 at 583.

<sup>54</sup> *Verge v. Somerville*, [1924] AC 496 at 499, cited with approval in *Guaranty Trust*, *supra* note 50 at 141.

<sup>55</sup> See, e.g., *Bowman v. Secular Society, Ltd.*, [1917] A.C. 406 at 442, concluding that "the Court has no means of judging whether a proposed change in the law will or will not be for the public benefit, and therefore cannot say that the gift to secure the change is a charitable gift"; and *Human Life International in Canada Inc. v. M.N.R.*, [1998] 3 C.T.C. 126, 98 D.T.C. 6196 (F.C.A.) at para. 12 (hereafter *Human Life International*), stating that "Courts should not be called upon to make such decisions as it involves granting or denying legitimacy to what are essentially political views: namely what are the proper forms of conduct, though not mandated by present law, to be urged on other members of the community?" For a conceptual discussion of the political purposes doctrine in the law of charities, see Abraham Drassinower, "The Doctrine of Political Purposes in the Law of Charities: A Conceptual Analysis," in Phillips et. al., eds., *Between State and Market*, *supra* note 37, 288.

<sup>56</sup> See, e.g., *Challenge Team v. Revenue Canada*, [2000] 2 C.T.C. 352, 2000 D.T.C. 6242 (F.C.A.).

<sup>57</sup> Canada Revenue Agency, T4063 "Registering a Charity for Income Tax Purposes" available at <http://www.cra-arc.gc.ca/E/pub/tg/t4063/README.html> (last updated 16 November 2001) at 8. See also *ibid.* at 6, stating that: "For an organization to be registered, its purposes have to fall within one or more of the following categories: the relief of poverty; the advancement of education; the advancement of religion; or certain other purposes that benefit the community in a way the courts have said are charitable."

<sup>58</sup> See, e.g., Canada Revenue Agency, "Registering a Charity for Income Tax Purposes" (30 January 1997), available at <http://www.cra-arc.gc.ca/tax/charities/policy/ces/ces-001-e.html> at para. 50 (explaining that "[a]n ostensibly charitable purpose can still fail if it does not meet the public benefit test" and emphasizing that there are "two sides" to this test: "how many people can benefit from the service offered by the charity, and whether the charity's services offer any tangible benefit to the community at large").



none of its purposes is political.<sup>59</sup> For this purpose, the prescribed form that applicants for charitable status must submit (Form T2050) requires them to identify the name and mailing address of the organization, its directors or trustees, its organizational structure, its programs and activities, financial information, and confidential information concerning the organization's business address or physical location, the physical location of books and records, the name and address of an authorized representative, contact information for directors or trustees, and financial statements for organizations that have operated for more than a year before applying for charitable status.<sup>60</sup>

In the leading judicial decision on this issue, the Federal Court of Appeal characterized the registration of charities as a "strictly administrative function,"<sup>61</sup> concluding on this basis that there is no obligation on the Minister to notify the applicant and invite representations or conduct a hearing before refusing its application for charitable status.<sup>62</sup> Notwithstanding this conclusion, the current administrative practice of the CRA is to send the applicant an Administrative Fairness Letter (AFL) explaining the reasons for denying charitable status, whereupon the applicant is given 90 days to respond.<sup>63</sup> Only if the applicant either does not respond or fails to respond satisfactorily to the AFL, does the CRA issue a Final Turn Down (FTD) letter refusing registered status.<sup>64</sup> Where an applicant has received a FTD letter, recent amendments to the ITA give the applicant 90 days to file a notice of objection with the Appeals Branch of the CRA,<sup>65</sup> which is required to assess the matter "with all due dispatch."<sup>66</sup> Where the Appeals Branch decides to uphold the decision to deny registration, the applicant must be notified by registered letter,<sup>67</sup>

<sup>59</sup> See, e.g., CRA, T4063, *supra* note 57 at 7 (stating that "political purposes are not charitable and an organization will not qualify for charitable registration if at least one of its purposes is political").

<sup>60</sup> Canada Revenue Agency, T2050 "Application to Register a Charity Under the *Income Tax Act*" available at <http://www.cra-arc.gc.ca/E/pbg/tf/t2050/README.html> (last modified 13 March 2002).

<sup>61</sup> *Scarborough Community Legal Services v. M.N.R.*, [1985] 1 C.T.C. 98, 85 D.T.C. 5102 (F.C.A.) at para. 10, *per* Marceau J.

<sup>62</sup> *Ibid.* at para. 11, *per* Marceau J.; and at para. 27, *per* Urie J. Dissenting, Heald J. concluded that the decision to deny registered status was a "quasi-judicial decision" such that it should have been given an opportunity to respond before its application was rejected. *Ibid.* at paras. 35 and 39.

<sup>63</sup> Canada Revenue Agency, *Registered Charities Newsletter*, No. 25 (Fall 2005) at 3, available at <http://www.cra-arc.gc.ca/E/pub/tg/charitiesnews-25/charitiesnews25-e.pdf>.

<sup>64</sup> *Ibid.*

<sup>65</sup> ITA, s. 168(4), added by S.C. 2005, c. 19, s. 38(1), applicable only to FTD letters issued by the CRA after 12 June 2005.

<sup>66</sup> ITA, s. 165(3).

<sup>67</sup> ITA, s. 149.1(22), added by S.C. 2005, c. 19, s. 35(6), applicable only after 12 June 2005.



and is given 30 days to file a notice of appeal to the Federal Court of Appeal.<sup>68</sup> The number of such appeals is minimal.<sup>69</sup>

In recent years, the number of applicants for registered charitable status has been approximately 3,500 to 4,000 per year, while the number of registrations each year has ranged from 2,281 in 2002 to 3,117 in 2005. As Table 1 illustrates, most cases in which applicants are not registered are attributable to abandoned or withdrawn applications rather than formal denials. In percentage terms, the number of registrations as a share of

**Table 1: Charities Applications and Registrations, 2002-2005**<sup>70</sup>

Year	New applications	Applications to re-register	Total applications	Administrative Fairness Letters	Denials	Registrations (%)
2002	3,017	540	3,557	1,054	56	2,281 (64.1)
2003	3,207	468	3,675	515	33	2,774 (75.5)
2004	3,043	445	3,488	482	19	2,592 (74.3)
2005	3,449	527	3,976	433	35	3,117 (78.4)

applications has increased from 64.1 percent in 2002 to 78.4 percent in 2005. As Table 2 indicates, the percentage of applicants obtaining registered status in 2002 is comparable to the registration rate prevailing in the late 1990s, while the percentage of applicants

**Table 2: Charities Applications and Registrations, 1992-1999**<sup>71</sup>

Year	Total applications	Registrations	Registration Rate (%)
1992-93	3,900	3,300	84.6
1993-94	4,400	3,350	79.5
1994-95	3,900	3,300	84.6
1995-96	5,000	4,500	90.0
1996-97	4,300	2,800	65.0
1997-98	4,800	3,000	62.5
1998-99	4,100	2,750	67.0

obtaining registered status in 2005 is closer to the registration rate in the early 1990s. The number of applications for charitable status during the period 2002-2005, however, is noticeably lower than the number of applications during the period 1992 to 1999. It is perhaps worth noting

<sup>68</sup> ITA, ss. 172(3)(a.1) and 180(1)(a).

<sup>69</sup> From 1987 to 1996, for example, the number of appeals averaged only eight per year. Lorne Sossin, "Regulating Virtue: A Purposive Approach to the Administration of Charities" in Phillips, et. al. *Between State and Market*, *supra* note 37, 373 at 387.

<sup>70</sup> Canada Revenue Agency, *Registered Charities Newsletters*, Nos. 15, 19, 23 and 27, available at <http://www.cra-arc.gc.ca/tax/charities/newsletters-e.html>.

<sup>71</sup> Monahan with Roth, *supra* note 16 at 12.

that a sharp decrease in the registration rate from 90 percent in 1995-96 to 65 percent in 1996-97 followed revocation of the Babbar Khalsa Society's charitable status in 1996, and that the decrease in applications for charitable status between 1999 and 2002 followed the attacks of September 11, 2001 and the enactment of the CRSIA later that year. Although the explanation for these shifts is not clear, they suggest that the CRA may have become more rigorous in its assessment of applications for registered status after the Babbar Khalsa Society's charitable status was revoked, which – together with the subsequent enactment of the CRSIA – may have led to fewer applications for registered status. If so, a more demanding regulatory regime may have reduced the number of organizations that would otherwise have obtained charitable status.

### 3. Maintaining Charitable Status

Once they are registered, charitable organizations and foundations are subject to several further requirements in addition to the basic requirement that their activities or purposes remain charitable under the legal test set out in the *Pemsel* case. According to subsection 149.1(14), registered charities must file an annual information return within 6 months of the end of their taxation year, containing sufficient information to enable the CRA to assess their activities. This return and accompanying worksheets require the charity to provide information on the charity's governing documents, directors or trustees, programs and activities, employee compensation, other financial information (assets, revenue and expenditures, including gifts to other qualified donees), and confidential information concerning the charity's physical location, the physical location of books and records, and the name and address of the person who completed the return.<sup>72</sup>

In addition to this annual reporting obligation, subsection 230(2) of the ITA imposes a further administrative requirement on registered charities to keep "records and books of account" at an address in Canada containing:

- (a) information in such form as will enable the Minister to determine whether there are any grounds for the revocation of registration under this Act;

---

<sup>72</sup> Canada Revenue Agency, T3010A "Registered Charity Information Return" available at <http://www.cra-arc.gc.ca/E/pbg/tf/t3010a/README.html> (last modified 16 June 2005).

- (b) a duplicate of each receipt containing prescribed information for a donation received by it; and
- (c) other information in such form as will enable the Minister to verify the donations to it for which a deduction or tax credit is available under this Act.

Where a charity fails to maintain adequate records and books of account, moreover, subsection 230(3) stipulates that “the Minister may require the person to keep such records and books of account as the Minister may specify, and that person shall thereafter keep records and books of account as so specified.”

In addition to these reporting and record-keeping requirements, registered charities must also refrain from engaging in various commercial activities,<sup>73</sup> and must satisfy a “disbursement quota” for expenditures on charitable activities or gifts to other qualified donees.<sup>74</sup> According to paragraphs 149.1(2)(a), 149.1(3)(a) and 149.1(4)(a), charitable organizations and public foundations may not carry on any business that is not a “related business” of the charity, while private foundations are prohibited from carrying on any business altogether. For the purpose of these provisions, the ITA defines a “business” quite broadly to include *inter alia* an undertaking of any kind whatever,<sup>75</sup> and judicial decisions have suggested that a related business must be closely connected to the activities or purposes of the charity and devote its moneys exclusively to these charitable activities or purposes.<sup>76</sup> According to paragraphs 149.1(2)(b), 149.1(3)(b) and 149.1(4)

<sup>73</sup> ITA, s. 149.1(2)(a) (charitable organization cannot carry on an unrelated business), ss. 149.1(3)(a), (c) and (d) (public foundation cannot carry on an unrelated business, cannot acquire control of any corporation, and cannot incur debts other than those specified), and ss. 149.1(4)(a), (b) and (c) (private foundation cannot carry on any business, cannot acquire control of any corporation, and cannot incur debts other than those specified).

<sup>74</sup> ITA, ss. 149.1(2)(b), (3)(b), and 4(b), and the definition of “disbursement quota” in ss. 149.1(1).

<sup>75</sup> ITA, s. 248(1) definition of “business”.

<sup>76</sup> *Alberta Institute on Mental Retardation v. The Queen*, [1987] 2 C.T.C. 70, 87 D.T.C. 3305 (F.C.A.) at para. 15 suggesting that the commercial activity at issue (collecting goods from donors and transferring them in exchange for a fee and expenses to a separate commercial enterprise which sold the goods for profit) had “a very close connection with the charity” because all of the revenues collected through the activity were allocated to the foundation’s charitable purposes. See also *Earth Fund / Fond pour la Terre v. M.N.R.*, [2003] 2 C.T.C. 10, 2003 D.T.C. 5015 (F.C.A.), rejecting the taxpayer’s argument that a proposed lottery business would constitute a related business solely because revenues from the lottery would be devoted exclusively to charitable purposes. See also the definition of “related business” in subsection 149.1(1) of the ITA, which extends the judicially-determined meaning to include “related business” to include “a business that is unrelated to the objects of the charity if substantially all persons employed by the charity in the carrying on of that business are not remunerated for that employment.” For a useful discussion of the advantages and disadvantages of allowing charities to engage in commercial activities, see Kevin Davis, “The Regulation of Social Enterprise” in Phillips, et. al., *Between State and Market*, *supra* note 37, 479.

(b), registered charities are generally required to spend 80 percent of the amount of receipted gifts from the previous year on charitable activities or gifts to other qualified donees.<sup>77</sup> Finally, paragraphs 149.1(3)(c) and 149.1(4)(c) stipulate that charitable foundations may not acquire control of any corporation, while paragraphs 149.1(3)(d) and 149.1(4)(d) state that charitable foundations may not incur debts, other than “debts for current operating expenses, debts incurred in connection with the purchase and sale of investments and debts incurred in the course of administering charitable activities”.

#### 4. Penalties and Sanctions

Until 2005, the only statutory remedy to deal with registered charities that failed to comply with the statutory and judicial requirements for maintaining their charitable status was revocation of this status. According to ITA subsection 168(1), the Minister may issue a notice of revocation where, among other circumstances, the registered charity:

- (a) applies to the Minister in writing for a revocation of its registration,
- (b) ceases to comply with the requirements of this Act for its registration as such,
- (c) fails to file an information return as and when required under this Act or a regulation, [or]
- (e) fails to comply with or contravenes ... section ... 230 [containing the requirement to maintain records and books of account].

Revocation of registered status is also authorized where the charity engages in prohibited commercial activities,<sup>78</sup> fails to satisfy its disbursement quota,<sup>79</sup> makes a gift of property to another charity in order to “unduly delay the expenditure of amounts on charitable activities”,<sup>80</sup> accepts a gift from another charity in order to enable the other charity to delay spending funds on charitable activities,<sup>81</sup> makes a false statement in order to obtain charitable status,<sup>82</sup> issues a receipt for a gift or a

<sup>77</sup> See the definition of “disbursement quota” in subsection 149.1(1) of the ITA. Under subsection 149.1(5), the Minister may, on application by the charity, reduce this percentage.

<sup>78</sup> ITA, ss. 149.1(2)(a), 149.1(3)(a), (c) and (d), and 149.1(4)(a), (b) and (c).

<sup>79</sup> ITA, ss. 149.1(2)(b), (3)(b), and (4)(b).

<sup>80</sup> ITA, s. 149.1(4.1)(a).

<sup>81</sup> ITA, s. 149.1(4.1)(b).

<sup>82</sup> ITA, s. 149.1(4.1)(c).



donation otherwise than in accordance with the ITA and the regulations or that contains false information,<sup>83</sup> or fails to comply with or contravenes enforcement measures in sections 231.1 to 231.5 of the ITA.<sup>84</sup> Although the ITA does not specify the manner in which the decision to revoke charitable status must be arrived at, judicial decisions have held that this process must be governed by principles of natural justice and procedural fairness such that “the Minister, before sending the notice, must first give to the person or persons concerned a reasonable opportunity to answer the allegations made against them.”<sup>85</sup> In addition, courts have emphasized that the decision to send a notice of revocation “must be arrived at in a manner enabling the Minister to create a record ... reflecting not only his point of view but also that of the organization concerned.”<sup>86</sup>

Where the CRA issues a notice of revocation, the charity has 90 days to file a notice of objection,<sup>87</sup> whereupon the Appeals Branch may reject or confirm the revocation.<sup>88</sup> If the Appeals Branch upholds the decision to revoke charitable status, the charity is given 30 days to file a notice of appeal to the Federal Court of Appeal,<sup>89</sup> which is required to hear and determine the appeal in a summary way.<sup>90</sup> For this purpose, judicial decisions have held that the charity bears the burden of disproving the assumptions of fact on which the decision to revoke charitable status is based.<sup>91</sup> Where the charity does not challenge the notice of revocation or the decision of the Appeals Branch or the Federal Court of Appeal upholds the decision to revoke charitable status, revocation becomes effective when a copy of the notice is published in the *Canada Gazette*.<sup>\*</sup> Where charitable status is revoked, section 188 gives the charity one year to expend its resources on charitable activities or transfer its property

---

<sup>83</sup> ITA, s. 168(1)(d).

<sup>84</sup> ITA, s. 168(1)(e).

<sup>85</sup> *Renaissance International v. M.N.R.*, [1982] C.T.C. 393, 83 D.T.C. 5024 (F.C.A.) at para. 17, *per Pratte J.* (hereafter *Renaissance International*). See also *Lord's Evangelical Church of Deliverance & Prayer of Toronto v. The Queen*, [2005] 1 C.T.C. 135, 2004 D.T.C. 6746 (F.C.A.) at para. 12.

<sup>86</sup> *Renaissance International*, *supra* note 85 at para. 16.

<sup>87</sup> ITA, s. 168(4), added by S.C. 2005, c. 19, s. 38(1), applicable to notices issued by the Minister of National Revenue after June 12, 2005.

<sup>88</sup> ITA, s. 165(3).

<sup>89</sup> ITA, ss. 172(3)(a.1) and 180(1)(a).

<sup>90</sup> ITA, s. 180(3).

<sup>91</sup> *Human Life International*, *supra* note 55 at para. 9, explaining that “the taxpayer is in the best position to provide information about his own affairs.”

<sup>92</sup> ITA, s. 168(2).

to an arm’s length charity, after which the value of any remaining assets is effectively forfeited to the Crown under a special penalty tax for this purpose.<sup>93</sup>

In recent years, the number of registered charities whose registration has been revoked has decreased from approximately 2,400 in 2002 to roughly 1,400 in 2005. As Table 3 demonstrates, most of these revocations are at the request of the charity or for failing to file an annual information return within 6 months of the end of its taxation year, with only a very few number of revocations for failing to comply with other requirements for registered status. Since the number of revocations for failing to file an information

**Table 3: Revocations of Charitable Status, 2002-2005<sup>94</sup>**

Year	Revocations by Request	Revocations for Failure to File Information Return	Revocations for Cause	Total Revocations
2002	800	1,599	5	2,404
2003	788	1,127	6	1,921
2004	709	1,261	8	1,978
2005	438	963	11	1,412

return on time exceeded 2,700 in 1999-2000,<sup>95</sup> it is apparent that revocations for this reason have decreased significantly in recent years.<sup>96</sup> In contrast, the number of revocations for cause is largely unchanged from the 1990s, when 33 charities had their status revoked on this basis from 1991 to 1996.<sup>97</sup>

As revocation is a severe sanction for relatively minor breaches such as the failure to file an information return on time, particularly if it leads to the imposition of the penalty tax under section 188, several studies in the

93 ITA, s. 188(1.1). See also the definition of a charity’s “winding-up period” in s. 188(1.2), the definition of an “eligible donee” in s. 188(1.3), s. 188(1) which deems the charity’s taxation year to end when it is issued a notice of revocation, and s. 189(6.1) which requires the charity to file a return and pay tax under s. 188(1.1) within a year after receiving the notice of revocation. In addition to these provisions, s. 188(2.1) permits the non-application of this penalty tax where the Minister abandons its intention to revoke the charity’s registered status or re-registers the charity within a year from when the notice of revocation is issued, or the charity has within the year filed all information returns that were required to be filed before that time and paid all amounts owing in respect of taxes, penalties and interest.

94 Canada Revenue Agency, *Registered Charities Newsletters*, Nos. 15, 19, 23 and 27, available at <http://www.cra-arc.gc.ca/tax/charities/newsletters-e.html>.

95 Canada Revenue Agency, *Registered Charity Newsletter*, No. 11 (Autumn 2001), available at <http://www.cra-arc.gc.ca/E/pub/tg/charitiesnews-11/news11-e.html>.

96 For 2005, this decrease is undoubtedly partly explained by the enactment of a \$500 penalty tax for late-filed information returns under subsection 188.1(6) of the ITA. See *infra* note 100 and accompanying text.

97 Panel on Accountability and Governance in the Voluntary Sector, *Building on Strength: Improving Governance and Accountability in Canada’s Voluntary Sector*, (February 1999) at 68.

late 1990s and early 2000s recommended that the federal government should enact intermediate sanctions and penalties as part of a more flexible approach to encourage regulatory compliance in the charitable sector.<sup>98</sup> In response to these recommendations, the federal government announced in the 2004 Federal Budget that it would amend the ITA to introduce “new, more effective sanctions that are more appropriate than revocation for relatively minor breaches of the *Income Tax Act*.”<sup>99</sup> Applicable to taxation years beginning after March 23, 2005, these intermediate penalties and sanctions allow the CRA to impose various penalty taxes and to suspend a charity’s privilege to issue charitable receipts where the charity fails to comply with specific statutory requirements.

Under new subsections 188.1(1) and (2), a registered charity that carries on an unrelated business (or any business in the case of a private foundation) is liable to a penalty tax equal to 5% of its gross revenue from the business or all of its gross revenue from the business if it was assessed for this penalty tax within the previous 5 years. Subsection 188.1(3) imposes a similar penalty tax on charitable foundations that acquire control of any corporation, equal to 5% of the amount of all dividends received from the corporation or the full amount of these dividends if it was assessed for this penalty tax within the previous 5 years. Subsection 188.1(6) imposes a penalty of \$500 on charities that fail to file an annual information return within 6 months of the end of its taxation year. Other penalty taxes apply where a registered charity confers an “undue benefit” on selected persons,<sup>100</sup> issues a receipt for a gift otherwise than in accordance with the ITA,<sup>101</sup> makes a false statement on a receipt,<sup>102</sup> or makes a gift of property

<sup>98</sup> See, e.g., OLRC, *supra* note 20, Vol. 1 at 378; Joint Tables, *Working Together: A Government of Canada Voluntary Sector Joint Initiative*, (August 1999) at 58-59; Panel on Accountability and Governance in the Voluntary Sector, *supra* note 97 at 72; Monahan with Roth, *supra* note 16 at 85; and Joint Regulatory Table, *Strengthening Canada’s Charitable Sector: Regulatory Reform*, (Ottawa: Voluntary Sector Initiative, March 2003).

<sup>99</sup> Canada, Department of Finance, *The Budget Plan 2004: A New Agenda for Achievement*, (Ottawa: Her Majesty the Queen in Right of Canada, 2004) at 351.

<sup>100</sup> ITA, s. 188.1(4), imposing a penalty tax on the charity equal to 105% of the amount of this benefit or 110% of the amount of the benefit if the charity was assessed for this penalty tax within the previous 5 years. For the purpose of this provision, s. 188.1(5) generally defines an “undue benefit” to include “a disbursement by way of a gift or the amount of any part of the income, rights, property or resources of the charity that is paid, payable, assigned or otherwise made available for the personal benefit of any person who is a proprietor, member, shareholder, trustee or settlor of the charity, who has contributed or otherwise paid into the charity more than 50% of the capital of the charity, or who does not deal at arm’s length with such a person or with the charity ....”

<sup>101</sup> ITA, ss. 118.1(7) and (8), imposing a penalty tax on the charity equal to 5% of the amount of the gift, or 10% of the amount of the gift if the charity was assessed for this penalty within the previous five years.

<sup>102</sup> ITA, s. 118.1(9), imposing a penalty tax equal to 125% of the amount of the gift for which the receipt is issued.

to another charity in order to “unduly delay the expenditure of amounts on charitable activities”.<sup>103</sup>

In addition to these penalties, new section 188.2 authorizes the Minister to suspend the charity’s tax-receipting privileges for one year where it has been penalized for a second time within five years for carrying on an unrelated business (or any business in the case of a private foundation) or conferring an undue benefit on a person,<sup>104</sup> where it incurs penalties exceeding \$25,000 for making false statements on receipts,<sup>105</sup> where it fails to maintain adequate records and books of account or fails to comply with other enforcement measures,<sup>106</sup> or if it may reasonably be considered that the charity has acted in concert with another charity whose receipting privileges have been suspended to accept a gift or transfer of property on behalf of that other charity.<sup>107</sup> During the one-year suspension period, moreover, the charity is not only precluded from issuing receipts for charitable gifts, but is also required, before accepting any gift, to inform the donor that its tax-receipting privileges have been suspended, that no deduction or credit may be claimed in respect of the gift, and that the gift is not a gift to a qualified donee.<sup>108</sup> To the extent that existing and potential supporters are given notice of the charity’s failings through this sanction, they may be in a position to persuade the charity to take remedial measures including the removal and replacement of directors or trustees, which the federal government could not accomplish directly given the constitutional limits of its jurisdictional authority.

Unlike the denial or revocation of charitable status, which can be appealed only to the Federal Court of Appeal, the imposition of these intermediate penalties and sanctions may be appealed to the Tax Court of Canada.<sup>109</sup> Where the Appeals Branch of the CRA confirms the assessment or suspension of receipting privileges, the charity has 90 days to file a notice of appeal to the Tax Court of Canada.<sup>110</sup> A charity may also apply to the

---

<sup>103</sup> ITA, s. 118.1(11), imposing a tax on each of the charities jointly and severally equal to 110% of the fair market value of the property.

<sup>104</sup> ITA, s. 188.2(1)(a) and (b).

<sup>105</sup> ITA, s. 188.2(1)(c).

<sup>106</sup> ITA, s. 188.2(2)(a).

<sup>107</sup> ITA, s. 188.2(2)(b).

<sup>108</sup> ITA, s. 188.2(3).

<sup>109</sup> ITA, s. 189(8).

<sup>110</sup> ITA, s. 169(1).



Tax Court of Canada for a postponement of the period for suspending receipting privileges,<sup>111</sup> which may grant such an application if “it would be just and equitable to do so.”<sup>112</sup>

As these intermediate penalties and sanctions apply only to taxation years beginning after March 23, 2005, empirical evidence on the use of these measures is not yet available. However, a significant decrease in the number of revocations in 2005 is likely attributable, in part at least, to the availability of these new penalties and sanctions.

## 5. The Charities Registration (Security Information) Act

In addition to the provisions of the ITA, the legal framework for registered charities also includes the CRSIA. First proposed as Bill C-16 on March 15, 2001,<sup>113</sup> the CRSIA was designed to demonstrate Canada’s commitment to the prevention of terrorist financing in accordance with resolutions adopted by the G-7 and the United Nations in 1996,<sup>114</sup> and Canada’s agreement to the *International Convention for the Suppression of the Financing of Terrorism* in February 2000,<sup>115</sup> and introduced in direct response to a specific recommendation by the Special Senate Committee on Security and Intelligence in January 1999 that:

... consideration be given to amending the *Income Tax Act* to allow Revenue Canada [now the Canada Customs and Revenue Agency] to deny charitable registration to

111 ITA, s. 188.2(4).

112 ITA, s. 188.2(5).

113 *An Act respecting the registration of charities and security information and to amend the Income Tax Act*, First Session, Thirty-seventh Parliament, 49-50 Elizabeth II, 2001 (First Reading, 15 March 2001) (hereafter “Bill C-16”).

114 G-7 Ministerial Conference on Terrorism (Paris, 30 July 1996), “Agreement on 25 Measures”, Resolution 19 (calling on all States to; “Prevent and take steps to counteract, through appropriate domestic measures, the financing of terrorists and terrorist organizations, whether such financing is direct or indirect through organizations which also have, or claim to have charitable, social or cultural goals, or which are also engaged in unlawful activities such as illicit arms trafficking, drug dealing, and racketeering.”); and General Assembly resolution 51/210 (17 December 1996), paragraph 3(f) (calling on all States to take steps “to prevent and counteract, through appropriate domestic measures, the financing of terrorists and terrorist organizations, whether such financing is direct or indirect through organizations which also have or claim to have charitable, social or cultural goals or which are also engaged in unlawful activities such as illicit arms trafficking, drug dealing and racketeering, including the exploitation of persons for purposes of funding terrorist activities ...”).

115 Adopted by the General Assembly of the United Nations in resolution 54/109 on 9 December 1999, and signed by Canada in February 2000.

any group on the basis of a certificate from the Canadian Security Intelligence Service that the group constitutes a threat to the security of Canada.<sup>116</sup>

After the terrorist attacks of September 11, 2001, Bill C-16 was incorporated into the federal government's anti-terrorism legislation as Part 6 of Bill C-36,<sup>117</sup> which was enacted in the autumn of 2001 and came into force on December 24, 2001.

According to subsection 2(1) of the CRSIA, the purpose of the legislation is threefold:

... to demonstrate Canada's commitment to participating in concerted international efforts to deny support to those who engage in terrorism, to protect the integrity of the registration system for charities under the *Income Tax Act* and to maintain the confidence of Canadian taxpayers that the benefits of charitable registration are made available only to organizations that operate exclusively for charitable purposes.<sup>118</sup>

In addition to demonstrating Canada's commitment to international efforts to prevent terrorist financing, therefore, the CRSIA also aims to protect the integrity of the registration system for charities under the ITA, and to maintain the confidence of the Canadian taxpayer that the benefits of charitable status are available only to organizations operating exclusively for charitable purposes.

Substantively, the key provisions of the CRSIA are subsections 4(1) and 8(1) and section 13. According to the first of these provisions, the Minister of Public Safety and Emergency Preparedness and the Minister of National

---

<sup>116</sup> *The Report of the Special Senate Committee on Security and Intelligence*, Chair: Hon. William M. Kelly, (January 1999), Recommendation 13 ("that consideration be given to amending the *Income Tax Act* to allow Revenue Canada [now the Canada Customs and Revenue Agency] to deny charitable registration to any group on the basis of a certificate from the Canadian Security Intelligence Service that the group constitutes a threat to the security of Canada.").

<sup>117</sup> *An Act to amend the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering) Act and other Acts, and to enact measures respecting the registration of charities, in order to combat terrorism*, First Session, Thirty-seventh Parliament, 49-50 Elizabeth II, 2001 (First Reading, 15 October 2001).

<sup>118</sup> CRSIA, s. 2(1).

Revenue may sign a certificate expressing their opinion, based on security or criminal intelligence information, that there are reasonable grounds to believe:

(a) that an applicant or registered charity has made, makes or will make available any resources directly or indirectly, to an entity that is a listed entity as defined in subsection 83.01(1) of the *Criminal Code*;

(b) that an applicant or registered charity made available any resources, directly or indirectly, to an entity as defined in subsection 83.01(1) of the *Criminal Code* and the entity was at that time, and continues to be, engaged in terrorist activities as defined in that subsection or activities in support of them; or

(c) that an applicant or registered charity makes or will make available any resources, directly or indirectly, to an entity as defined in subsection 83.01(1) of the *Criminal Code* and the entity engages or will engage in terrorist activities as defined in that subsection or activities in support of them.

According to subsection 8(1), a certificate that is determined to be reasonable under the process outlined below is “conclusive proof that, in the case of an applicant, it is ineligible to become a registered charity or, in the case of a registered charity, that it does not comply with the requirements to continue to be a registered charity.” According to section 13 of the CRSIA, a certificate is “effective for a period of seven years beginning on the first day it is determined to be reasonable” unless it is cancelled earlier. On this basis, therefore, the CRA may deny registered status to an applicant or revoke the charitable status of a registered charity where the applicant or registered charity is subject to a certificate that is determined to be reasonable under the CRSIA.

The process for determining whether a certificate issued under subsection 4(1) is reasonable is set out in sections 5 to 7 of the CRSIA. According to subsection 5(1), as soon as the Minister of Public Safety and Emergency Preparedness and the Minister of National Revenue have signed a certificate, the Minister of Public Safety and Emergency Preparedness or a person authorized by this Minister shall cause the applicant or

registered charity to be served with a copy of the certificate and a notice informing it that “the certificate will be referred to the Federal Court not earlier than seven days after service and that, if the certificate is determined to be reasonable, the applicant will be ineligible to become a registered charity or the registration of the registered charity will be revoked, as the case may be.” In addition, subsection 5(5) stipulates that seven days after this service “or as soon afterwards as is practicable,” the Minister of Public Safety and Emergency Preparedness or a person authorized by this Minister shall file a copy of the certificate with the Federal Court for it to make a determination under section 7 and cause the applicant or registered charity to be served with a notice informing it of the filing of the certificate. In order to preserve the confidentiality of this process, subsection 5(3) permits the applicant or registered charity to apply to the Federal Court for an order directing that “the identity of the applicant or registered charity not be published or broadcast in any way” except in accordance with the CRSIA, or that “any documents to be filed with the Federal Court in connection with the reference be treated as confidential.”<sup>119</sup>

According to section 7 of the CRSIA, the Chief Justice of the Federal Court or a judge of the Court designated by the Chief Justice shall “determine whether the certificate is reasonable on the basis of the information and evidence available,”<sup>120</sup> and “quash a certificate if the judge is of the opinion that it is not reasonable.”<sup>121</sup> For the purpose of this determination, section 6 provides for an informal hearing process,<sup>122</sup> in which the judge is required to examine the information and evidence on which the certificate is based in private,<sup>123</sup> provide the applicant or registered charity with a summary of the information or evidence that “enables it to be reasonably informed of the circumstances giving rise to the certificate,”<sup>124</sup> and provide the applicant or registered charity with an opportunity to be heard.<sup>125</sup> Section 6 also provides for the confidentiality of information and

---

<sup>119</sup> See also CRSIA, s. 5(4), stipulating that an order on an application under subsection 5(3) is “not subject to an appeal or review by any court at the instance of a party to the application.”

<sup>120</sup> CRSIA, s. 7(1).

<sup>121</sup> CRSIA, s. 7(2).

<sup>122</sup> CRSIA, s. 6(a) and (c), stipulating that the judge shall hear the matter and “with all matters as informally and expeditiously as the circumstances and considerations of fairness and natural justice permit”.

<sup>123</sup> CRSIA, s. 6(d).

<sup>124</sup> CRSIA, s. 6(h).

<sup>125</sup> CRSIA, s. 6(i).



evidence if the judge concludes that its disclosure would be “injurious to national security or endanger the safety of any person” if disclosed,<sup>126</sup> and waives the ordinary rules of evidence by allowing the judge to “receive into evidence anything that, in the opinion of the judge is reliable and appropriate, even if it is inadmissible in a court of law” and to “base the decision on that evidence.”<sup>127</sup>

Where a judge determines that a certificate is reasonable under subsection 7(1) of the CRSIA, subsection 8(2) stipulates that the determination is “final and ... not subject to appeal or judicial review.” For this purpose, subsections 168(3) and 172(3.1) of the ITA exclude these determinations from the normal appeals processes that are otherwise available when charitable status is denied or revoked – both to the Appeals Branch and to the Federal Court of Appeal. Where a certificate is determined to be reasonable under subsection 7(1), the Minister of Public Safety and Emergency Preparedness is required “without delay” to cause the certificate to be published in the *Canada Gazette*,<sup>128</sup> thereby making the name of the applicant or registered charity public information.

Notwithstanding a determination that a certificate is reasonable, section 10 of the CRSIA provides for a review of the certificate by the Minister of Public Safety and Emergency Preparedness and the Minister of National Revenue if the applicant or former registered charity believes that there has been a “material change in circumstances” since the determination under subsection 7(1). For this purpose, the Ministers may consider “any submission made by the applicant or former registered charity” and “any information that is made available” to them,<sup>129</sup> and decide whether there has or has not been a material change in circumstances.<sup>130</sup> If the Ministers

<sup>126</sup> CRSIA, s. 6(b) and (h), stipulating that “the judge shall ensure the confidentiality of the information on which the certificate is based and of any other evidence that may be provided to the judge if, in the opinion of the judge, its disclosure would be injurious to national security or endanger the safety of any person” and that the summary of the information or evidence that the judge provides to the applicant or registered charity shall “not include anything that in the opinion of the judge would be injurious to national security or endanger the safety of any person if disclosed”. See also s. 6(e) and (g), stipulating that the judge shall, when requested by the Minister of Public Safety and Emergency Preparedness or the Minister of National Revenue, “hear all or part of the information or evidence in the absence of the applicant or registered charity named in the certificate and their counsel if, in the opinion of the judge, its disclosure would be injurious to national security or endanger the safety of any person” and that this information or evidence “shall not be included in the summary of the information or evidence that enables it to be reasonably informed of the circumstances giving rise to the certificate, but that does not include anything that in the opinion of the judge would be injurious to national security or endanger the safety of any person”.

<sup>127</sup> CRSIA, s. 6(j).

<sup>128</sup> CRSIA, s. 8(3).

<sup>129</sup> CRSIA, s. 10(3).

<sup>130</sup> CRSIA, s. 10(5).

decide that there has not been a material change in circumstances, the CRSIA requires them to deny the application<sup>131</sup>; if the Ministers decide that there has been a material change of circumstances, on the other hand, the CRSIA requires them to determine whether there are reasonable grounds as provided in subsection 4(1) and accordingly to continue the certificate in effect or cancel the certificate as of the date of the decision.<sup>132</sup> If the Ministers do not make a decision within 120 days after receiving the application, the CRSIA provides that the certificate is cancelled at the end of that 120-day period.<sup>133</sup> Where a certificate is cancelled for either of these reasons, the Minister of Public Safety and Emergency Preparedness is required to cause to be published in the *Canada Gazette* notice of the cancellation “in a manner that mentions the original publication of the certificate.”<sup>134</sup>

If the Ministers decide that there has been no material change in circumstance or that there has been such a change but that a reasonable ground in subsection 4(1) still applies, the applicant or registered charity may apply for a review by the Federal Court in accordance with the procedure set out in section 6 of the CRSIA.<sup>135</sup> In this circumstance, subsection 11(3) stipulates that the Court shall refer the application to the Minister if it determines that a material change of circumstance has occurred, and subsection 11(4) states that the certificate is cancelled if the Court determines that there are not reasonable grounds under subsection 4(1). As with a determination under subsection 7(1) a determination under section 11 is not subject to appeal or judicial review.<sup>136</sup> If the certificate is cancelled by reason of a determination by the Federal Court, notice of the cancellation must be published in the *Canada Gazette*.<sup>137</sup>

To date, no certificates have been issued under the CRSIA.<sup>138</sup> Indeed, according to then Commissioner of the Canada Customs and Revenue

131 CRSIA, s. 10(5)(a).

132 CRSIA, s. 10(5)(b).

133 CRSIA, s. 10(6).

134 CRSIA, s. 12.

135 CRSIA, ss. 11(1) and (2).

136 CRSIA, s. 11(5).

137 CRSIA, s. 12.

138 Special Senate Committee on the Anti-Terrorism Act, *Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the Anti-Terrorism Act*, (February 2007) at 60, reporting on statements by the Minister of Public Safety and the Minister of Justice and Attorney General that “to date, the power to issue a certificate under the CRSIA has not been used.” See also House of Commons Standing Committee on Public Safety and National Security Subcommittee on the Review of the Anti-Terrorism Act (Subcommittee on the Review of the Anti-Terrorism Act), *Rights, Limits, Security: A Comprehensive Review of the Anti-Terrorism Act and Related Issues*, (March 2007) at 34, reporting that “[t]o the Subcommittee’s knowledge, no certificates have been issues under this legislation.”

Agency (CCRA), Michel Dorais:

... if there was an organization that had some link with terrorist organizations, it would probably be faulting on other grounds, so before we'd get to that point the process of decertification would already be launched on the grounds of money not flowing for charity purposes or books not being kept properly.<sup>139</sup>

As well, since the onus of proof under an ordinary revocation proceeding falls on the charity to disprove the assumptions of fact on which the decision to revoke is based, it may be easier to revoke registered status on this basis than under the CRSIA, notwithstanding the "reasonable belief" standard on which revocation under the CRSIA may be based.

Despite the fact that no certificates have been issued under the CRSIA, however, the CRA maintains that CRSIA provides "an effective deterrent" and a "prudent reserve power to address cases of terrorism" when "classified information may be needed to establish an organization's support for terrorism."<sup>140</sup> For charitable organizations and their advocates, on the other hand, the CRSIA has created "a chill on charitable activities in Canada, as charities hesitate to undertake programs that might expose them to violation of anti-terrorism legislation and the possible loss of their charitable status."<sup>141</sup>

### III. Information Collection and Sharing

In order to ensure that charities satisfy and adhere to the legal and administrative requirements for registered status under the ITA, applicants for charitable status must file an application identifying the name and address of the organization, its directors or trustees, its organizational structure, its programs and activities, and financial information,<sup>142</sup> and registered charities must file an annual information return containing the

<sup>139</sup> Subcommittee on Public Safety and National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness, 38<sup>th</sup> Parliament, 1<sup>st</sup> Session, Evidence (18 May 2005) 1545 (statement by Mr. Michel Dorais, Commissioner, Canada Customs and Revenue Agency).

<sup>140</sup> *Ibid.* at 1535. See also *ibid.* at 1555, stating that "these powers can deter some organizations which may consider registering as charities in Canada for terrorist purposes."

<sup>141</sup> Terrance S. Carter, "Charities and Compliance with Anti-Terrorism Legislation: The Shadow of the Law" (2004), 19:1 *The Philanthropist* 43 at 44.

<sup>142</sup> Form T2050, *supra* note 60.

names of the charity's directors or trustees, a description of the charity's programs and activities, and financial information reporting the charity's assets, revenue and expenditures, including gifts to other qualified donees.<sup>143</sup> The ITA also grants the CRA broad investigatory powers, allowing authorized persons to

(a) inspect, audit or examine the books and records of a taxpayer and any document of the taxpayer or of any other person that related or may relate to the information that is or should be in the books or records of the taxpayer ..., and

(b) examine ... any property or process of, or matter relating to, the taxpayer or any other person, an examination of which may assist the authorized person in ... ascertaining the information that is or should be in the books or records of the taxpayer ...,

and for these purposes to

(c) ... enter into any premises or place where any business is carried on, any property is kept, anything is done in connection with any business or any books or records are or should be kept, and

(d) require the owner or manager of the property or business and any other person on the premises or place to give the authorized person all reasonable assistance and to answer all proper questions relating to the administration or enforcement of this Act, and for that purpose, require the owner or manager to attend at the premises or place with the authorized person.<sup>144</sup>

Although the CRA generally does not need to obtain search warrants to exercise these extensive audit powers,<sup>145</sup> courts have held that they must be obtained if the predominate purpose of the investigation is to determine whether criminal liability exists.<sup>146</sup> In these circumstances, the

<sup>143</sup> ITA, s. 149.1(14). The information return for this purpose is form T3010A, *supra* note 69.

<sup>144</sup> ITA, s. 231.1(1).

<sup>145</sup> Where the premises or place of business referred to in paragraph 231.1(1)(c) is a dwelling house, subsections 231.1(2) and (3) require the Minister to apply to a judge of the superior court for a warrant authorizing entry.

<sup>146</sup> *R. v. Jarvis* (2002), 3 S.C.R. 757.



CRA must obtain a search warrant based on the traditional criminal law standard that there are reasonable grounds to believe that an offence has been committed and that the search will reveal evidence of this offence.

In addition to these investigatory powers, the CRA may, for any purpose related to the administration or enforcement of the ITA, serve notice on any person, requiring the person to provide “any information or additional information” or “any document.”<sup>147</sup> Where it obtains a warrant from a superior court judge, the CRA may also “enter and search any building, receptacle or place for any document or thing that may afford evidence as to the commission of an offence under this Act” and “seize the document or thing.”<sup>148</sup>

In recent years, as Table 4 demonstrates, the CRA has audited between about 350 and 600 registered charities each year, which represents a tiny fraction of the roughly 80,000 charities that are registered under the ITA. Although the number of audits

**Table 4: Audits of Registered Charities, 2002-2005**<sup>149</sup>

Year	Audits
2002	475
2003	356
2004	367
2005	596

increased significantly in 2005, this figure was only slightly higher than the 576 audits conducted ten years earlier,<sup>150</sup> when the number of registered charities was closer to 70,000.<sup>151</sup>

In addition to the information that it receives from annual information returns and investigations, the CRA also reviews intelligence assessments, briefs and classified information provided by the RCMP and CSIS, as well as publicly available information, to determine whether charities

<sup>147</sup> ITA, s. 231.2(1).

<sup>148</sup> ITA, s. 231.3(1). According to subsection 231.3(3), a judge may issue the warrant where “the judge is satisfied that there are reasonable grounds to believe that (a) an offence under this Act was committed; (b) a document or thing that may afford evidence of the commission of the offence is likely to be found; and (c) the building, receptacle or place specified in the application is likely to contain such a document or thing.”

<sup>149</sup> Canada Revenue Agency, *Registered Charities Newsletters*, Nos. 15, 19, 23 and 27, available at <http://www.cra-arc.gc.ca/tax/charities/newsletters-e.html>.

<sup>150</sup> Sossin, “Regulating Virtue,” *supra* note 69 at 388.

<sup>151</sup> Monahan with Roth, *supra* note 16 at 11.

are involved with or lend support to terrorist organizations.<sup>152</sup> Recent amendments to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* also authorize FINTRAC to disclose information to the CRA where there are reasonable grounds to suspect that the information is relevant to investigating or prosecuting a money laundering offence or a terrorist financing offence and reasonable grounds to suspect that the information is relevant to determining whether an applicant is eligible for charitable status under the ITA or a registered charity has ceased to comply with the requirements for this status.<sup>153</sup> Although the CRA does not obtain information from revenue authorities and charities regulators in other countries, it hopes to be able to conclude such arrangements in the future.<sup>154</sup>

As a general rule, the ITA provides for the confidentiality of taxpayer information, stipulating in subsection 241(1) that, except as expressly authorized, no official shall:

- (a) knowingly provide, or knowingly allow to be provided, to any person any taxpayer information;
- (b) knowingly allow any person to have access to any taxpayer information; or
- (c) knowingly use any taxpayer information otherwise than in the course of the administration or enforcement of this Act ...

and in subsection 241(2) that “no official shall be required, in connection with any legal proceedings, to give or produce evidence relating to any taxpayer information.” For the purposes of these rules, the ITA defines an “official” generally as any person employed by or engaged by or on behalf of Her Majesty in right of Canada or a province, and “taxpayer information” as “information of any kind and in any form relating to one

---

<sup>152</sup> Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's Security Activities*, (Ottawa: Her Majesty the Queen in Right of Canada, 2006) at 190. See also Subcommittee on Public Safety and National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness, *supra* note 139 at 1630 (statement by Ms. Elizabeth Tromp, Director General, Charities Directorate, Policy and Planning Branch, Canada Customs and Revenue Agency).

<sup>153</sup> *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, *supra* note 6, s. 55(3)(c), added by S.C. 2006, c. 12, s. 26(4), assented to 14 December 2006.

<sup>154</sup> Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *supra* note 152 at 190.

or more taxpayers" that is either obtained by or on behalf of the CRA for the purposes of the ITA or prepared from this information, excluding "information that does not directly or indirectly reveal the identity of the taxpayer to whom it relates."<sup>155</sup>

Notwithstanding these general rules regarding the confidentiality of taxpayer information, other provisions allow for the disclosure of taxpayer information in criminal proceedings under any Act of Parliament or in legal proceedings related to the enforcement of the ITA,<sup>156</sup> where a warrant to investigate a threat to the security of Canada is issued under subsection 21(3) of the *Canadian Security Intelligence Service Act*,<sup>157</sup> or where a judge issues an order regarding an investigation into a terrorism offence under subsection 462.48(3) of the *Criminal Code*.<sup>158</sup> As well, another provision authorizes the Minister to "provide to appropriate persons any taxpayer information relating to imminent danger of death or physical injury to any individual."<sup>159</sup> In practice, however, the CRA considers the threshold for disclosing information under this "imminent danger" provision very high, and such disclosures are reportedly "rare and limited."<sup>160</sup>

In addition to these provisions, the ITA contains three further exceptions to the general confidentiality rules that apply specifically to registered charities and applicants for charitable status. First, under subsection 241(3.2) of the ITA, an official may provide to "any person" various kinds of information relating to a person that was "at any time" a registered charity, including: (a) a copy of the charity's governing documents, including its statement of purpose; (b) any information contained in its application for charitable status; (c) the names of persons who at any time were its directors and the periods during which they were directors; (d) a copy of the notification of the charity's registration, including any conditions and warnings; (e) a copy of any notice of revocation or annulment sent to the charity if its registration has been revoked or annulled; (f) financial statements required to be included in the annual information return; (g) a copy of any notice imposing a penalty tax under section 188.1 of the ITA or suspending the charity's privilege to issue receipts under section 188.2; and (h) information filed by the charity in support of an application

---

<sup>155</sup> ITA, s. 241(10).

<sup>156</sup> ITA, s. 241(3).

<sup>157</sup> R.S.C. 1985, c. 23. See ITA, s. 241(4)(e)(iv).

<sup>158</sup> *Supra* note 5. See ITA, s. 241(4)(e)(v).

<sup>159</sup> ITA, s. 241(3.1).

<sup>160</sup> Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *supra* note 152 at 191.

for special status or exemption under the ITA.<sup>161</sup> Announced in the 1997 Federal Budget and enacted in 1998, this provision was introduced in order to “improve donors’ access to information about charities, and provide for greater transparency with regard to charity’s affairs” in order to “increase self-discipline in the charitable sector, and empower donors to play a better role in monitoring the sector” and to enable the revenue authorities to “better address concerns that have been raised regarding those few charities that are not meeting the requirements for charitable status.”<sup>162</sup> While the disclosure rule applies to charities that are currently registered or were registered “at any time”, however, it does not apply to charities that have merely applied for registered status.

Second, under paragraph 241(1)(f.1) of the ITA, an official may provide any taxpayer information to another official for the purposes of the administration and enforcement of the CRSIA. Enacted as part of the federal government’s anti-terrorism legislation in autumn 2001,<sup>163</sup> this provision effectively allows the CRA to share any taxpayer information for the purpose of assessing whether there are reasonable grounds to believe that a registered charity or applicant for registered status has made, makes or will make its resources available to a terrorist organization. Where the official to whom this taxpayer information is disclosed is a member of CSIS or the RCMP, moreover, new subsection 241(9.1) allows this official to use or communicate to another official of CSIS or the RCMP any of this information other than “designated donor information” for the purpose of:

(a) investigating whether an office may have been committed, ascertaining the identity of a person or persons who may have committed an offence, or prosecuting an offence, which offence is

(i) described in Part II.1 of the Criminal Code [terrorism offences], or

(ii) described in section 462.31 of the *Criminal Code* [laundering proceeds of crime], if that investigation, ascertainment or prosecution is related to an investigation, ascertainment or prosecution in respect of an offence described in Part II.1 of that Act, or

<sup>161</sup> ITA, s. 241(3.2), added by S.C. 1998, c. 19, s. 65(1), applicable on Royal Assent, June 18, 1998.

<sup>162</sup> Canada, Department of Finance, Budget 1997: Building the Future for Canadians, (Ottawa: Her Majesty the Queen in Right of Canada, 1997) at 199

<sup>163</sup> S.C. 2001, c. 11, s. 33, coming into force on December 24, 2001.



(b) investigating whether the activities of any person may constitute threats to the security of Canada, as defined in section 2 of the *Canadian Security Intelligence Service Act*.

For the purpose of these provisions, the ITA protects the confidentiality of Canadian donors by defining “designated donor information” as information regarding a gift to a charity or applicant for charitable status that “directly or indirectly reveals the identity of the donor” (other than a donor who is not resident in Canada and is neither a citizen of Canada nor subject to Canadian income tax under Part I of the ITA).<sup>164</sup> Subsection 241(9.1) and the definition of “designated donor information” were recently enacted as part of a series of amendments to federal legislation dealing with terrorist financing.<sup>165</sup>

Finally, new subsection 241(9), which was enacted in 2006 together with other amendments to federal legislation dealing with terrorist financing,<sup>166</sup> allows an official to provide to an official of CSIS, the RCMP or FINTRAC three kinds of information. Paragraph (a) provides for the disclosure of “publicly accessible charity information” which the ITA defines as the information of a charity or applicant for charitable status that is listed in subsection 241(3.2), information other than designated donor information that is contained in a charity’s annual information return, and information that is prepared from this information.<sup>167</sup> More significantly, paragraph (b) allows for the disclosure of “designated taxpayer information” if there are reasonable grounds to suspect that the information would be relevant to:

(i) an investigation by the Canadian Security Intelligence Service of whether the activity of any person may constitute threats to the security of Canada, as defined in section 2 of the *Canadian Security Intelligence Service Act*,

(ii) an investigation of whether an offence may have been committed under

<sup>164</sup> ITA, s. 241(10), added by S.C. 2006, c. 12, s. 45(3), assented to December 13, 2006..

<sup>165</sup> *An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the Income Tax Act and to make a consequential amendment to another Act*, S.C. 2006, c. 12, s. 45, assented to December 13, 2006.

<sup>166</sup> *Ibid.*

<sup>167</sup> ITA, s. 241(10), added by S.C. 2006, c. 12, s. 45(3), assented to December 13, 2006.

(A) Part II.1 of the *Criminal Code* [terrorism offences], or

(B) section 462.31 of the *Criminal Code* [laundering proceeds of crime], if that investigation is related to an offence under Part II.1 of that Act, or

(iii) the prosecution of an offence referred to in subparagraph (ii).

For the purpose of this provision, the ITA defines “designated taxpayer information” as taxpayer information (other than designated donor information) of a registered charity or an applicant for charitable status that is:

(a) in respect of a financial transaction

(i) relating to the importation or exportation of currency or monetary instruments by the charity or applicant, or

(ii) in which the charity or applicant has engaged a person to whom section 5 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* applies [listing persons who are required to keep records and report suspicious transactions],

(b) information provided to the Minister by the Canadian Security Intelligence Service, the Royal Canadian Mounted Police or the Financial Transactions and Reports Analysis Centre of Canada,

(c) the name, address, date of birth and citizenship of any current or former director, trustee or like official, or of any agent, mandatary or employee, of the charity or applicant,

(d) information submitted by the charity or applicant in support of an application for registration as a registered charity that is not publicly accessible charity information,

(e) publicly available, including commercially available databases, or

(f) information prepared from publicly accessible charity

information and information referred to in paragraphs (a) to (e).<sup>168</sup>

As well, paragraph (c) provides for the disclosure of information setting out the reasonable grounds for suspicion under paragraph (b) to the extent that those grounds rely on publicly accessible charity information or designated taxpayer information. Like subsection 241(9.1), therefore, subsection 249(9) protects the confidentiality of Canadian donors by excluding designated donor information from the kinds of information that may be disclosed. Unlike subsection 241(9.1), on the other hand, which depends on an initial disclosure of taxpayer information for the purposes of the administration and enforcement of the CRSIA, subsection 241(9) permits the routine disclosure of publicly accessible charity information and the disclosure of designated taxpayer information whenever there are reasonable grounds to suspect that the information may be relevant to the investigation of a threat to the security of Canada or an investigation or prosecution of any of the terrorism offences in the *Criminal Code*.

#### IV. Evaluation

In order to evaluate Canada's legal framework for limiting the use or misuse of charitable organizations for terrorist financing, it is useful to begin by recognizing two important considerations on which this evaluation should be based. First, as Canadian experience with the Babbar Khalsa Society and Sikh temple funds sadly demonstrates, charitable organizations can be vulnerable to manipulation by individuals and groups who seek to take advantage of the legitimacy and fiscal benefits that these organizations obtain through registered status in order to finance terrorist activities.<sup>169</sup> For this reason, effective supervision and regulation of registered charities is essential – not only to constrain opportunities for terrorist financing, but also to protect the integrity of the legal regime governing the conferral

<sup>168</sup> *Ibid.*

<sup>169</sup> In this respect, see Financial Action Task Force on Money Laundering, *Combating the Abuse of Non-Profit Organisations: International Best Practices*, (11 October 2002), available at <http://www.fatf-gafi.org/dataoecd/39/19/34033761.pdf>, describing non-profit organizations as “a crucial weak point” in the global struggle to stop terrorist financing at its source. See also Financial Task Force on Money Laundering, *Interpretative Note to Special Recommendation VII: Non-Profit Organizations*, (15 February 2006), available at <http://www.fatf-gafi.org/ataoecd/16/6/36174688.pdf>, at para. 2, explaining that terrorist organizations have “taken advantage” of various characteristics of non-profit organizations (NPOs), including the public trust that they enjoy, in order to “infiltrate the sector and misuse NPO funds and operations to cover for or support terrorist activity.”

of tax benefits under the ITA, and to safeguard the interests of donors who expect that their charitable contributions will be used for legitimate purposes.<sup>170</sup> For this reason, as well, it is commendable that Canada has joined international efforts to prevent terrorist financing through charitable organizations – for example, by signing the *International Convention for the Suppression of the Financing of Terrorism* in February 2000,<sup>171</sup> and participating in the Financial Action Task Force on Money Laundering (FATF), an inter-governmental body that was established in order to develop and promote national and international policies to combat money laundering and terrorist financing.<sup>172</sup> For all of these reasons, moreover, this report fully endorses the declared purposes of the CRSIA to “demonstrate Canada’s commitment to participating in concerted international efforts to deny support to those who engage in terrorism,” to “protect the integrity of the registration system for charities under the *Income Tax Act*” and to “maintain the confidence of Canadian taxpayers that the benefits of charitable registration are made available only to organizations that operate exclusively for charitable purposes.”<sup>173</sup>

Second, it is also important to recognize the central role that the charities play nationally and internationally, as key participants in domestic economies and the global economy,<sup>174</sup> as organizations that foster international solidarity and provide humanitarian and development assistance to people in some of the most troubled and disadvantaged parts of the world,<sup>175</sup> as institutions that promote social inclusion and build social capital,<sup>176</sup> and as vehicles through which citizens experience each of the four fundamental freedoms guaranteed by the Canadian

---

170 See, e.g., Financial Task Force on Money Laundering, *Interpretative Note to Special Recommendation VII*, *supra* note 169 at para. 1, explaining that misuse of non-profit organizations for terrorist financing “not only facilitates terrorist activity but also undermines donor confidence and jeopardises the very integrity of NPOs.”

171 *Supra* note 115.

172 The FATF was established by the G-7 Summit held in Paris in 1989, when it was given the responsibility to examine money laundering techniques and trends, review action which has already been taken at the national and international level, and suggest further measure to combat money laundering. After the attacks of September 11, 2001, the mandate of the FATF was expanded to include measures to prevent terrorist financing. The FATF currently includes 33 member countries and 2 observers. See [http://www.fatf-gafi.org/pages/0,2966,en\\_32250379\\_32235720\\_1\\_1\\_1\\_1\\_1\\_0\\_0.html](http://www.fatf-gafi.org/pages/0,2966,en_32250379_32235720_1_1_1_1_1_0_0.html).

173 CRSIA, s. 2(1).

174 FATF, *Combating the Abuse of Non-Profit Organisations: International Best Practices*, *supra* note 169 at para. 5.

175 Nolan Quigley and Belinda Pratten, *Security and Civil Society: The Impact of Counter-Terrorism Measures on Civil Society Organisations*, (London: National Council for Voluntary Organisations, 2007), available at <http://www.ncvo-vol.org.uk/?id=3906> at 7.

176 See, e.g., *ibid.* at 9.



*Charter of Rights and Freedoms*,<sup>177</sup> as well as the practical challenges that many charities face as small organizations with unpaid volunteers,<sup>178</sup> and the very small number of charities in Canada and other countries that have actually had any connection with terrorist activities.<sup>179</sup> For these reasons, as advocates for the charitable sector have emphasized, charities should generally be seen as valuable allies in the global struggle against terrorism, rather than suspects.<sup>180</sup> More importantly, for the purposes of this report, government supervision and regulation of the charitable sector should be proportionate and risk-based – emphasizing capacity-building and best practices to prevent the use or misuse of charitable organizations for terrorist financing, ensuring transparency and self-regulation to the greatest extent possible, scrutinizing transactions and organizations that pose the greatest risks for terrorist links, and limiting more serious regulatory sanctions to the rare instances where charities provide support to terrorist organizations.<sup>181</sup>

Turning to the specific legal regime for registered charities in Canada, recent initiatives demonstrate increased emphasis on the proportionate and risk-based regulatory approach described in the previous paragraph. Through its Charities Partnership and Outreach Program, for example, the CRA funds education and training aimed at improving the capacity of registered charities to comply with statutory and administrative requirements for registration under the ITA.<sup>182</sup> The CRA has also issued guidelines for charities operating outside Canada,<sup>183</sup> though it has yet to issue its own guidelines on best practices to prevent the use and abuse

<sup>177</sup> *Constitution Act 1982, Schedule B to Canada Act 1982 (U.K.)*, s. 2, listing: “(a) freedom of conscience and religion; freedom of thought, belief, opinion and expression ...; (c) freedom of peaceful assembly; and (d) freedom of association.”

<sup>178</sup> See *supra* notes 44-45 and accompanying text.

<sup>179</sup> In Canada, for example, no certificates have been issued under the CRSIA and the CRA has provided information to the RCMP’s Anti-Terrorist Financing Group in relation to the certificate process only “on a very few occasions.” Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *supra* note 152 at 190. In the United Kingdom, the Charity Commission’s Operational Guidance on Charities and Terrorism reports that “the incidence of charity involvement with terrorist organizations is very rare.” Charity Commission, *Operational Guidance: Charities and Terrorism*, (28 January 2003), available at <http://www.charity-commission.gov.uk/supportingcharities/ogs/g096.asp>.

<sup>180</sup> See, e.g., Quigley and Pratten, *supra* note 175, emphasizing that the charitable sector should be viewed as “part of the solution” to global terrorism, not part of the problem. See also OMB Watch, *Safeguarding Charity in the War on Terror: Anti-terrorism Financing Measures and Nonprofits*, (October 2005) at 11, concluding that “the government should recognize the positive role nonprofits play in the campaign against international violence and terrorism.”

<sup>181</sup> See, e.g., Quigley and Pratten, *supra* note 175 at 17. See also FATF, *Combating the Abuse of Non-Profit Organisations: International Best Practices*, *supra* note 169 at para. 5.

<sup>182</sup> *Supra* note 26. For 2006 to 2008, funding priorities under this program emphasize compliance with statutory and administrative requirements for international operations as well as fundraising, receipting and the maintenance of records and books of account.

<sup>183</sup> *Supra* note 45.

of terrorist organizations for terrorist financing.<sup>184</sup> Amendments to the ITA that authorize the public disclosure of information about registered charities have greatly increased transparency within the charitable sector, enabling donors and members to play a much greater role monitoring the sector and initiating regulatory responses.<sup>185</sup> As well, recent increases in audit rates make it more likely that organizations with potential links to terrorists will be identified, though audit rates remain very small and appear to be lower than they were in the mid-1990s.<sup>186</sup> Since many audits are initiated by public complaints, however, increased transparency and public disclosure likely permit more targeted audits. Amendments authorizing information exchanges with CSIS, the RCMP and FINTRAC also enable these organizations and the CRA to devote greater attention to organizations and individuals where risks of terrorist links appear to be greatest.<sup>187</sup> Finally, the introduction of intermediate penalties and sanctions in 2005 provides for a range of regulatory responses that are more proportionate to different categories of non-compliance than the ultimate sanction of revocation.<sup>188</sup> They also provide signals to existing and potential donors that a charity may not be complying with relevant laws, enabling these individuals to put additional pressure on the charity to take remedial measures.

These measures go a long way toward preventing the use and misuse of charitable organizations for terrorist financing that occurred in Canada with the Babbar Khalsa Society and Sikh temple funds. In the case of the Babbar Khalsa Society, current provisions for the exchange of information might well have caused the CRA to deny registered status before it was granted, on the grounds that the organization's purposes or activities were not exclusively charitable according to the legal definition adopted in the *Pemsel* case.<sup>189</sup> Alternatively, the public disclosure of information on registered charities under subsection 241(3.2) of the ITA

<sup>184</sup> Canada Revenue Agency, "Charities in the International Context," available at <http://www.cra-arc.gc.ca/tax/charities/international-e.html> (last modified 10 April 2006), explaining that "[i]t can be difficult to be certain exactly what rules apply, which guidelines to follow, or if there are best practices that could inform how charitable activities should be carried out." In contrast to the CRA, both the FATF and the U.S. Department of the Treasury have issued international best practices guidelines to prevent the use or misuse of charitable organizations for terrorist financing. See FATF, *Combating the Abuse of Non-Profit Organisations: International Best Practices*, *supra* note 169; and U.S. Department of the Treasury Anti-Terrorist Financing Guidelines: *Voluntary Best Practices for U.S.-Based Charities*, available at <http://www.ustreas.gov/press/releases/docs/tocc.pdf>.

<sup>185</sup> See ITA, s. 241(3.2), discussed at *supra* notes 161-162, and accompanying text.

<sup>186</sup> See *supra*, text accompanying notes 150-151.

<sup>187</sup> See *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, *supra* note 6, s. 55(3)(c), discussed at *supra* note 152-153 and accompanying text; and ITA, ss. 241(1)(f.1), 241(9), and 241(9.1), discussed at *supra* notes 163-169 and accompanying text.

<sup>188</sup> ITA, ss. 188.1 and 188.2, discussed at *supra* notes 100-112 and accompanying text.

<sup>189</sup> *Supra* note 53 and accompanying text.

might have created pressure for revocation much earlier than 1996. Since this rule limits the disclosure of information to charities that are or were registered, however, it does not enable members of the public to monitor the organizations that apply for charitable status, as a consequence of which public pressure can only be brought to bear once the charity has obtained registered status. For this reason, subsection 241(3.2) might reasonably be amended to authorize the disclosure of information relating to a person who was at any time either a registered charity or an applicant for registered status.

In the case of Sikh temple funds, increased transparency and information exchange could have produced a measured regulatory response, beginning with a formal audit and the imposition of intermediate penalties and sanctions designed to encourage self-regulation by members of the affected temples, culminating if necessary in the ultimate sanction of revocation and the application of the penalty tax under section 188 of the ITA. Since the federal government's constitutional jurisdiction over charities extends only to the conferral of fiscal benefits under the ITA, however, other regulatory responses such as the removal and replacement of directors or trustees would have required action by the provincial Attorney-General.<sup>190</sup> Although publicity might have prompted such a response, provincial governments have been reluctant to exercise their jurisdictional authority in this area. For this reason, federal and provincial governments should consider alternative arrangements to facilitate a more robust regulatory regime for charities, involving at the very least the exchange of information about charities and more ambitiously the possible delegation of federal and provincial authority over charities to an administrative agency that could exercise broad supervisory and regulatory powers. Since federal regulation applies only to charities that seek or obtain registered status, moreover, not charities that do not apply for registered status, nor other nonprofit and voluntary organizations, federal and provincial governments should also consider what joint initiatives might be taken to establish a more extensive regulatory regime for charities and other nonprofit and voluntary organizations, irrespective of their registered status under the ITA.

As part of the legal and administrative framework for registered charities

---

<sup>190</sup> See the explanation of the constitutional framework governing charities in Canada at *supra*, Part I. This is in contrast to the much broader powers of the U.K. Charity Commission, which were deployed to suspend and then remove Abu Hamza from his position in the Finsbury Park Mosque. See Mark Sidel, "Terrorist Financing and the Charitable Sector: Law and Policy in the United Kingdom, the United States, and Australia" Research Paper Prepared for Commission of Inquiry into the Investigation of the Bombing of Air India (2007) at 8.



in Canada, the CRSIA has a very limited role to play. Since support for terrorist activities cannot be construed as charitable under any of the categories contained in the legal definition, denial or revocation of registered status can generally be accomplished under the ordinary rules of the ITA, without having to resort to the CRSIA. As then Commission of the CCRA explained to the Subcommittee on Public Safety and National Security of the House of Commons Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness in May 2005:

... if there was an organization that had some link with terrorist organizations, it would probably be faulting on other grounds, so before we'd get to that point the process of decertification would already be launched on the grounds of money not flowing for charity purposes or books not being kept properly.<sup>191</sup>

The effect of the CRSIA, therefore, is not to permit the denial or revocation of registered status for charities that support terrorist activities, but to establish a different process for the determination of charitable status where security considerations suggest that the information on which this determination is based should remain confidential.

While confidentiality is undoubtedly a legitimate concern in this and other legal responses to terrorism, the CRSIA has four significant deficiencies. First, the grounds on which registered status may be denied or revoked are extremely broad, applying where the applicant or registered charity "has made, makes or will make available any resources directly or indirectly" to a listed terrorist entity, "made available any resources directly or indirectly" to an entity that was at the time or continues to be engaged in terrorist activities, or "makes or will make available any resources directly or indirectly" to an entity that engages or will engage in terrorist activities.<sup>192</sup> Second, the CRSIA requires no knowledge or fault on the part of the applicant or registered charity, and does not even allow for a due diligence defence for charities that adopt reasonable measures to ensure that resources are not made available to terrorists. Third, the extent of confidentiality under the CRSIA may be such that the charity is unable to mount a serious adversarial challenge to the information on which a certificate is based.<sup>193</sup> Finally, in contrast to the intermediate penalties

---

<sup>191</sup> *Supra* note 139.

<sup>192</sup> CRSIA, s. 4(1).



and sanctions that were added to the ITA in 2005,<sup>194</sup> the only sanction under the CRSIA is the denial or revocation of charitable status.<sup>195</sup>

Because the grounds for denying or revoking registered status are so broad, the CRSIA is likely to be applied either selectively or not at all. More seriously, the combination of this broad language with the absence of any knowledge or fault requirement or a due diligence defence, is apt to deter charities from engaging in international operations, particularly in conflict zones, where it is often difficult to monitor the use of charitable resources by agents and contractors. This is particularly so to the extent that the CRSIA results in revocation of charitable status and the potential application of the penalty tax under section 188 of the ITA.<sup>196</sup> For these reasons, the CRSIA might reasonably be amended to include a knowledge or fault requirement in subsection 4(1), stipulating that the applicant or registered charity either “knowingly or negligently” makes, made, or will make available resources to a listed terrorist entity or an entity that it “knew or ought to have known” engages in a terrorist activity.<sup>197</sup> In addition to this knowledge or fault requirement, the CRSIA might also be amended by introducing a due diligence defence, according to which a certificate shall be quashed where the applicant or registered charity demonstrates that it has exercised due diligence to ensure that its resources are not available to terrorists.<sup>198</sup> For this purpose, moreover, the CRA might develop best practice guidelines that charities could rely upon in order to demonstrate due diligence.<sup>199</sup> Finally, where a charity’s resources are made available to terrorists despite its best efforts, the CRSIA might also

---

<sup>193</sup> For a critical evaluation of procedural aspects of the CRSIA, see Lorne Sossin, “The Intersection of Administrative Law with the Anti-Terrorist Bill” in Daniels, et. al., *supra* note 5, 419 at 422-25. For a recent evaluation of similar confidentiality provisions in the context of *Criminal Code* anti-terrorism provisions, see *Charkaoui v. Canada*, 2007 S.C.C. 9.

<sup>194</sup> ITA, ss. 188.1 and 188.2, discussed at *supra* notes 100-112 and accompanying text.

<sup>195</sup> CRSIA, s. 8(1).

<sup>196</sup> *Supra* note 93 and accompanying text.

<sup>197</sup> The Subcommittee on the Review of the Anti-Terrorism Act makes a similar recommendation in its Final Report, *supra* note 138 at 38, but limits this knowledge requirement to the entity engaging in terrorist activities, without also including the availability of resources to this entity. According to the Report: “The Subcommittee believes that it is unfair to penalize an organization when it had no reason to believe that its resources were assisting an entity engaged in terrorism.”

<sup>198</sup> The Subcommittee on the Review of the Anti-Terrorism Act makes the same recommendation, *ibid.* at 36, despite suggesting that “a close reading” of subsection 4(1) of the CRSIA indicates that “for a certificate to be issued, the applicant or registered charity must have consciously and intentionally undertaken activities that directly or indirectly support terrorist activity.” The current author does not share this interpretation of the provision.

<sup>199</sup> The Subcommittee on the Review of the Anti-Terrorism Act makes a similar recommendation, *ibid.* at 36.

be amended to allow for intermediate penalties and sanctions like those in sections 188.1 and 188.2 of the ITA. As well, an alternative procedure might be devised to give charities a more meaningful opportunity to challenge the information on which a certificate is based.

## V. Conclusion

Over the past decade, a number of changes have significantly improved the effectiveness of Canada's legal framework to constrain the use or misuse of charitable organizations for terrorist financing. Amendments to the ITA authorizing the public disclosure of information about registered charities greatly increase the probability that regulatory non-compliance will be discovered and addressed either through self-regulation by members and donors or through regulatory responses by federal or provincial authorities. Information sharing between the CRA and other government agencies such as CSIS, the RCMP and FINTRAC also increases the likelihood that organizations that make resources available to terrorists will be identified so that regulatory responses may be initiated. At the same time, the recent introduction of intermediate penalties and sanctions allows for a more measured regulatory response based on the degree of non-compliance. Finally, the CRSIA allows for the use of confidential information to deny registered status where a charity makes resources available to terrorists. Were these measures in place in the late 1980s and early 1990s, it is difficult to imagine that the Babbar Khalsa Society would have been able to obtain charitable status or retain this status until 1996, and difficult to imagine that Sikh temple funds would have been misused for terrorist financing.

Notwithstanding these improvements in Canada's legal framework, there are four areas in which further improvements might be made. First, in order to prevent organizations with links to terrorism from obtaining charitable status in the first place, subsection 241(3.2) of the ITA might be amended to authorize the disclosure of information about applicants for charitable status as well as persons who are or were registered. Second, administrative information sharing arrangements might be expanded to include exchanges with revenue authorities and other government agencies in other countries. Third, in order to ensure a proportionate response to the risk of terrorist financing through charitable organizations, the CRSIA should be amended to introduce a knowledge or negligence requirement, a due diligence defence, and intermediate penalties. Finally, federal and provincial governments should cooperate to establish a more

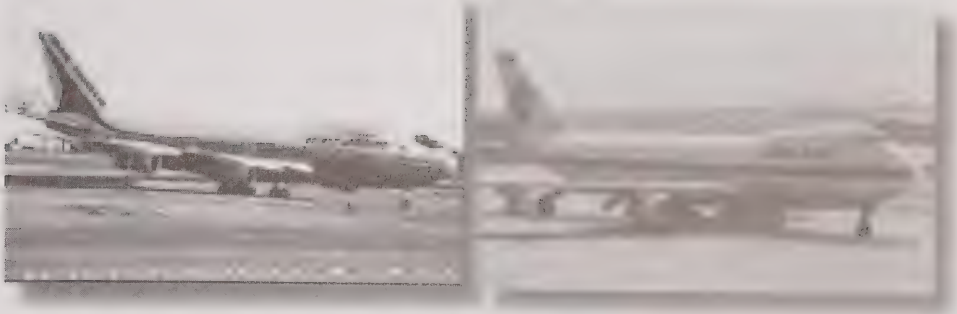
robust regulatory regime for charities and other nonprofit and voluntary organizations, including a greater range of regulatory responses than tax-based penalties and sanctions, and extending to organizations that might be used or misused for terrorist financing but do not apply for charitable status.

David G. Duff ([www.law.utoronto.ca/faculty/duff](http://www.law.utoronto.ca/faculty/duff)) is an Associate Professor at the University of Toronto Faculty of Law, which he joined in 1996. He holds an LL.M. from Harvard and an LL.B. from the University of Toronto, master's degrees in political theory from the University of Toronto and economics from York University, and a B.A. (Honours) from Queen's University.

Prior to joining the Faculty, Professor Duff was a tax associate at the Toronto office of Stikeman, Elliott. He was also employed as a researcher with the Ontario Fair Tax Commission from 1991 to 1993 and as a tax policy analyst with the Ontario Ministry of Finance in 1993-1994. He is a member of the Law Society of Upper Canada and was called to the Bar in 1996. He has been a visiting scholar at the Faculty of Law of Oxford University, at the University of Sydney Law Faculty, and at the Faculty of Law at McGill University.

Professor Duff's teaching and research interests are in the areas of tax law and policy, environmental taxation, comparative and international taxation, statutory interpretation, and distributive justice. He has published numerous articles in the areas of taxation, environmental policy, as well as tort and family law, and a textbook/casebook on *Canadian Income Tax Law*. Among these publications are several articles on the tax treatment of charities and charitable contributions and on charities and terrorist financing. The focus of his current research is distributive justice and tax policy.





## Canadian Airport Security Review

### Introduction

The aviation industry has received a considerable input of money since the crash of Air India Flight 182, the events of September 2001 and the Report of the Standing Senate Committee on National Security and Defence entitled, "The Myth of Security at Canada's Airports."<sup>1</sup> First, in the form of improvements in the realm of passenger baggage reconciliation and secondly by the fact that the industry has seen significant changes as regards the presence and supervision of security equipment and personnel.

Legislation passed immediately after the 9/11 tragedy transferred the security function of passenger and carry on baggage screening from the airline carriers to the new Canadian Air Transport Security Authority (CATSA) which was created as part of a comprehensive, \$2.2 billion package of air security initiatives contained in the December 2001 budget. CATSA came into force on April 1, 2002, through Bill C-49.<sup>2</sup> CATSA is a Crown corporation based in the National Capital Region. It reports to Parliament through the Minister of Transport. Its mission is to protect the public by securing critical elements of the air transportation system as assigned by the government. In addition, 59 additional Transport Canada Security Inspectors across the five regions in the National Capital Region were hired, funding for aircraft security modifications of up to \$30 million and a one time payment for increased police presence and security at airports (up to 20 million) were put into place.<sup>3</sup>

<sup>1</sup> Report of the Standing Senate Committee on National Security and Defence. (January 2003). *The Myth of Security at Canada's Airports*. Second Session Thirty Seventh Parliament.

<sup>2</sup> *Canadian Air Transport Security Act Statutes of Canada 2002 c.9.*

<sup>3</sup> Ibid.



This paper will focus on the breaches of airport security that led to the 1985 bombing of Air India Flight 182 and whether those breaches have been adequately addressed. I will also describe the events leading to the 1988 bombing of Pan Am Flight 103 over Lockerbie. There are significant cost effective measures that can be taken to prevent tragedies of this nature in the future. This paper will support the premise that the key to efficient aviation security is on the ground. Admittedly, every available tool in the tool box needs to be integrated into an overall security network, but the passenger baggage reconciliation is a solvable problem. The paper will review the procedures in place both before and after the Air India and Pan Am flights and some of the equipment available to screen passengers and baggage.

### **Air India Flight 182- 22/23 June 1985 Background**

On June 16, 1985, a caller using the telephone number of the Ross Street Sikh Temple in Vancouver booked a single ticket for A. Singh to depart Vancouver via CP Flight 003 to Tokyo on June 22, 1985. The departing passenger was to connect with Air India Flight 301 in Tokyo. This ticket was never picked up because a change in plans was made to target two aircraft instead of just one. Three days later, a telephone caller spent a considerable time with a CP Air booking agent looking for suitable connecting flights to New Delhi for two people traveling in different directions from Vancouver. One passenger was to travel to New Delhi via Air India Flight 182 from Toronto and another via Air India Flight 301 in Tokyo. Three days later, and two days before the bombings, a man of East Indian descent wearing a saffron turban, arrived at the downtown ticket office of CP Air carrying cash. He paid for two tickets. Both were registered under the last name "Singh." One ticket was for passenger M. Singh flying from Vancouver to Toronto on June 22, 1985 via CP Air Flight 060 and connecting with Air India Flight 182 in Toronto. The other passenger, L. Singh, was to fly to Tokyo on the same day via CP Flight 003 and connecting with Air India Flight 301 from Narita to Bangkok. He paid \$3005 cash for the two consecutively numbered tickets.<sup>4</sup> On June 22, 1985, a clean-shaven, well-dressed man lined up at counter 26 at Vancouver International Airport at around 8 a.m. and insisted the clerk direct-connect his bag with Air India Flight 182 in Toronto. The clerk originally said she could not do that because he was wait-listed. He was told that he was confirmed on Canadian Pacific Flight 060 to Toronto but was waitlisted for Air India Flight 181 Toronto to Montreal and then Air India Flight 182 from Montreal

<sup>4</sup> Bob Rae. (2005). *Lessons to be Learned on Outstanding Questions with Respect to the Bombing of Air India Flight 182*, Ottawa: Air India Review Secretariat. .

to Delhi. The airline employee that checked the bag recalled that the man was particularly insistent that his bag be interlined all the way to Air India Flight 182. This was eventually done and there was no reconciliation check between records of bags and passengers before the flight took off; contrary to airline rules. The passenger argued and clerk relented. While his bag was boarded on the flight leaving from Vancouver, M. Singh did not board the aircraft but had a bomb in his checked baggage. At around 11 a.m. another Sikh lined up at the same counter to check in his bag for CP Flight 003 to Tokyo. Additionally, another airline agent checked in two pieces of luggage at the Vancouver International Airport containing a bomb. L. Singh's bag took off but the passenger did not board the flight. At exactly 6.13 (a.m.) GMT, a bag off-loaded from CP Flight 003 at Tokyo's Narita Airport exploded as it was being taken to waiting Air India Flight 301. The first suitcase exploded inside the baggage terminal at Tokyo's Narita Airport while being transferred to the Air India flight. Two baggage handlers are killed and four were wounded. Exactly 55 minutes later, the other bag, a dark-brown hard-sided Samsonite suitcase, exploded in the forward cargo hold of Air India Flight 182 as it approached the coast of Ireland. The flight disintegrated at altitude and the wreckage was scattered along a nine-mile swath of the ocean at 6,000 feet. The voice recorder showed there had been a loud bang aboard the aircraft. It also picked up the hissing sound of the fuselage opening up and a scream. The data recorders showed everything was normal on the aircraft until the explosion. The data recorder also showed a momentary control input by the pilot as he desperately tried to re-configure the aircraft. Some passengers actually survived the 747's fall from 31,000 feet only to drown in the frigid waters of the Atlantic. The attack killed 329 people, including 82 children. Among the victims are 280 Canadian citizens, mostly born in India or of Indian descent.

After the Air India crash, Canada was the first ICAO member to require passenger baggage reconciliation on international flights, which was later extended to domestic flights as well. Canada also initiated comprehensive background checks for airport workers and removal of baggage coin lockers from major airports. Cameras in and around security checkpoints were also banned. The current measures for checked baggage in 1985 were generally the same as existed prior to 2001 except that checked baggage on flights to the US must now be screened using a combination of explosive detections machines, physical means and conventional x-rays. By Jan 2006, all checked baggage from Canadian airports for any



destination is subject to screening, however, the gap regarding cargo remains unchanged.<sup>5</sup>

## **Pan Am Flight 103- Lockerbie, Scotland- 21 December 1988- Background**

The actual aircraft for Pan American Flight 103, a Boeing 747, N739PA, had originated in San Francisco. Many of the passengers arrived from Frankfurt, West Germany, on a Boeing 727, which had been positioned next to the Boeing 747. The passengers were transferred with their baggage to N739PA, which was to fly to New York. After a 6-hour turn around, the aircraft left Heathrow airport at 6:04 PM with 243 passengers and a crew of 16 on board. The aircraft exploded over Lockerbie, Scotland, and fell to the ground in pieces, killing 11 more innocent souls on the ground. Major portions of the wreckage fell over the town of Lockerbie and to the East. Smaller debris was strewn along two trails, the longest, which extended approximately 130 kilometers to the coast of England. The impact of the crashing plane was so strong that the British Geological Survey recorded a seismic event measuring 1.6 on the Richter scale.

Responsibility was originally thought to fall on the Popular Front for the Liberation of Palestine because of radio cassette bombs discovered in the hands of the PFLP-GC prior to the bombing. Many intelligence analysts were convinced that the Iranians were retaliating for the accidental shoot down of one of their commercial carriers. The latest evidence, however, indicated Muammar Khadaffi was really responsible. Law enforcement later discovered a significant clue. A link was established between an obscure case involving the arrest of Mohammed Marzouk and Mansour Omran Saber, both Libyan Intelligence agents, at Dakar, Senegal, airport in 1988 and the Lockerbie explosive device. It turns out they had in their possession 20 pounds of Semtex plastic, TNT explosives, weapons and some triggering devices. One of the triggering devices matched a microchip fragment from the Pan Am bomb. The circuit board fragment recovered from the crash was actually part of a sophisticated electronic timer. Senegalese authorities discovered the same type in the possession of the two Libyan terrorists who had been arrested in February 1988. Meister et Bollier, a Swiss electronics firm, specially manufactured the timers, designated as MST-13, and all 13 timers had been delivered to the Libyans. The perpetrators had made use of the Czech-made explosive

<sup>5</sup> Indian Kirpal Report, Report Of The Court Investigating Accident To Air India Boeing 747 Aircraft VT ETO, "Kanishka" On 23rd June 1985.) and (Canadian Aviation Bureau Aviation Occurrence, Air India Boeing, 747-237B VT-EFO Report)

and very powerful Semtex. A double detonator device was used. The first trigger was activated by barometric pressure, which in turn activated a timing device. The actual bomb was encased in a Toshiba radio-cassette player. The terrorists were able to obtain and attach an appropriately marked Air Malta tag that enabled the luggage to circumvent baggage security measures and to be directly routed to the Pan Am feeder flight.

Forensic experts identified the bag that contained the bomb as a brown, hard-sided Samsonite suitcase. One of the defendants, Al-Megrahi, arrived in Valletta's Luqa airport, with the other defendant, Fhimah from Libya on the evening of 20 December 1988. Because Fhimah had been the former manager of the Maltese airport he had somehow retained full access to the airport. Scottish investigators traced the clothing that had been packed in the bag to a shop in Malta. Frankfurt airport records show that an unaccompanied bag was routed from the Air Malta Flight 180 to Frankfurt where it was eventually loaded onto the Pan Am Flight 103 feeder flight, as per perfectly legal procedures in effect at the time.

Other safety and security issues were also involved. Apparently a telephone threat, received from an anonymous caller on December 5 1988, at the American Embassy in Helsinki, Finland, warned of the impending disaster. The caller claimed a Finnish woman would carry a bomb aboard a Pan Am flight from Frankfurt to the US sometime during the next two weeks. US State Department sent out diplomatic traffic notifying its own personnel. Even though notice again was disseminated to all US consulates and embassies, since Finnish police determined it was a hoax, the information was not passed onto the FAA. The procedure of non-disclosure, which emerged from this incident and was persistently raised by the families of the victims, posed the question of exactly who should be advised in the event of threat information. The recommendation of the US President's Commission on Aviation Security and Terrorism in May 1990 was in favor of public notification of threats to civil aviation. However, security officials and the air carriers had reaffirmed an overall policy of nondisclosure.

The Lockerbie incident also raised the issue of passenger/baggage reconciliation. The President's Commission reported and concluded that passenger/baggage reconciliation is a bedrock component of any heightened security program. In 1988, Pan Am was x-raying all interlined bags rather than identifying and physically searching unaccompanied interline bags. Pan Am additionally claimed it had FAA approval to do this even though the FAA insisted it did not. Investigation disclosed the

presence of an extra bag when the flight left Frankfurt, which had not been physically searched. It is unclear whether the bag had been x-rayed. This is important for Air India where the x ray machine broke down and investigators could not determine whether the bag was x rayed or not. Based on the recommendations of the Gore commission, US carriers were required to institute a strict bag matching policy to remove the baggage of any passenger who failed to actually board an aircraft. Canada did not institute these procedures until after the Air India crash. The process became fairly routine in the US, however not all overseas airlines and airports meet the requirements of such a program.

Many airlines now use a computer link between the luggage tag and the boarding pass; scanning the boarding pass when the passenger begins to actually board the aircraft and matching the individual to each piece of luggage. Again, not every airline in every city has implemented these procedures. If the airline determines that a passenger with checked baggage does not board the flight, the bags are located and removed from the flight, sometimes requiring significant delays. The process is known in the trade as "originating" passenger/baggage match. Meaning it is accomplished at the beginning of the first leg of the flight. Unfortunately, the process does not consider any bag that may already be in the cargo hold of the aircraft. If a person exits the aircraft during a stop over, the baggage may continue on without the passenger on board. Consequently, an originating passenger/baggage match system is really only a partial bag match if it does not reconcile the baggage and passengers already on board the aircraft after each and every stop. This, of course, could be administratively quite costly and time consuming. Checking interline bags would add additional costs to already expensive airline security measures.<sup>6</sup>

### **Comparisons and Dissimilarities: Procedures/Security Measures/Equipment Air India**

A check of CP Air's records and interviews with passengers indicates that the persons identifying themselves as M. and L. Singh did not board these respective flights. Air India Flight 181 from Frankfurt arrived at Toronto on 22 June 1985 at 1430 EDT (1830 GMT) and was parked at gate 107 of Terminal 2. All passengers and baggage were removed from the aircraft and processed through Canada Customs. Passengers continuing on the flight to Montreal were given transit cards, and on this flight, 68 cards were

<sup>6</sup> AAIB Aircraft Accident Report No 2/90, Pan Am 103, 22 December 1988, Boeing 747; NAVAVNSAFECEN Investigation 69-67.



handed out. These transit passengers are required to claim their luggage and proceed through Canadian Customs. Prior to entering the public area, there is a belt which is designated for interline or transit baggage. Transit passengers deposit their luggage on this belt which carries it to be reloaded on the aircraft. This baggage was not subjected to X-ray inspection as it was presumed to have been screened at the passengers' overseas departure point. When the transit passengers checked in to proceed to Montreal, their carry-on baggage was subjected to the normal security checks in place on this date. Passenger and baggage security checks were conducted by Burns International Security Services Ltd. and all passengers and baggage processing for both off-loading and on-loading was handled by Air Canada staff. It should be noted that some passengers from India book flights to Montreal with their intended destination being Toronto. The reason is that the fare to Montreal was cheaper and therefore some passengers get off the flight in Toronto, claim their luggage and leave without reporting a cancellation of the trip to Montreal. It has been established that 65 of the 68 transit passengers re boarded the flight to Montreal. Air India personnel were in charge for the overall operation at Toronto regarding the unloading and loading of both passengers and cargo. Although the actual work was performed by various companies under contract, Air India personnel oversaw the operation. The Air India station manager was away on vacation on 22 June 1985. The evidence does not clearly establish who had been assigned to replace the station manager and assume his duties. Furthermore, Air Canada had been storing an engine that had failed on a previous Air India flight from Toronto on 8 June 1985. Air Canada received a message from Air India stating that the failed engine was to be mounted as a 5th pod on Flight 181/182 on 22 June 1985. Due to problems with loading the 5th pod and component parts, the departure was delayed from 1835 EDT (2235 GMT) to 2015 EDT (0015 GMT, 23 June).<sup>7</sup>

CP Air Flight 060 arrived in Toronto at 1610 EDT (2010 GMT) and docked at gate 44, Terminal 1. A number of passengers on this flight were interlined to other flights including passenger M. Singh wait-listed on Air India Flight 181/182. It has been established that this passenger did not board Flight CP 060 but did check baggage onto the flight. This baggage was to be interlined to the Air India flight departing from Terminal 2. In this case, CP Air employees would have off-loaded all baggage from CP 060 and deposited the baggage at Racetrack 6 on the ring road of Terminal 1 to be

---

<sup>7</sup> AirDisaster.com, Special Report: Air India Flight 182: <http://www.airdisaster.com/special/special-ai182.shtml>.



transported to the Air Canada sorting room at Terminal 2. Consolidated Aviation Fuelling and Services (CAFAS) is a company which is contracted to pick up and deliver baggage from one terminal to the other. The CAFAS driver on duty at the time recalls picking up a bag from a CP Air flight originating in Vancouver and destined for Air India at Terminal 2. As this piece of luggage did not turn up as found luggage, it is deduced that normal practice was followed, and the luggage was interlined and loaded on AI 181/182. MEGA International Air Cargo is a firm that handled air cargo and containers for Air India. Since the flight was carrying a 5th engine and component parts, no commercial cargo could be loaded at Toronto. MEGA delivered the engine component parts to be loaded in the cargo compartment by Air Canada employees. Later, MEGA received two diplomatic bags and delivered these to the aircraft. The bags were loaded into the valuable goods container. These bags were not subjected to X-ray or any other security checks.

All checked-in baggage for AI 181/182 was to be screened by an X-ray machine which was located in Terminal 2 at the end of international belt number 4. This location would permit all baggage from the check-in counters and interline carts to be fed through the X-ray machine before being loaded. It has been established that this machine worked intermittently for a period of time and stopped working during the loading process at about 1700 EDT (2100 GMT). Rather than opening the bags and physically inspecting them, the Burns security personnel performing the X-ray screening were told by the Air India security officer to start using the hand-held PD sniffer. One Burns security officer checked the bags with the sniffer while another put stickers on the bags and forwarded them. The security officer forwarding the baggage recalls the sniffer making short beeping noises not long whistling ones. The security officer who used the sniffer claims it never went off, and the only time any sound was made was when it was turned on and off. At those times, it would emanate a short beep. Burns International Security had a contract with Air India for the security of the aircraft while it was docked. The security arrangements contracted from Burns were as follows:

- security at the bridge door leading to the aircraft;
- security inside the aircraft from the time the passengers disembarked upon flight arrival until flight departure;
- security guards assigned the physical inspection of all carry-on baggage in the departure room; and
- security guards in the international baggage make-up room conducting screening of baggage using an X-ray machine and a hand-held PD-4 sniffer.

The statements taken from Burns security personnel in Toronto indicated that a significant number of personnel, including those handling passenger screening, had never had the Transport Canada passenger inspection training program or, if they had, had not undergone refresher training within 12 months of the previous training. As a result of official requests made by Air India in early June 1985 for increased security for Air India flights, the RCMP provided additional security as follows:

- one member in a marked police motor vehicle patrolling the apron area;
- one member in a marked police motor vehicle parked under the right wing from time of arrival until push-back;
- one member on foot patrol at Air India check-in counter; and
- one member at the loading bridge during boarding.

In addition, all RCMP members working in that particular area of Terminal 2 were aware of the Air India flight and would check in with the assigned personnel during their patrols in the area of the aircraft and check in/boarding lounges. Uniformed members were to patrol and monitor security within the airport premises. Passenger check-in was handled for Air India by Air Canada under contract with Air India. The check-in included passengers originating in Toronto and interline passengers but did not include the transit passengers to Montreal. The check-in passengers were numbered using a security control sheet in accordance with instructions from Air India; however, the check-in and interline baggage was not numbered, and no attempt was made to correlate baggage with passengers. Hence, any unaccompanied interline baggage would not have been detected. The flight and cabin crew had been in Toronto for the week prior to this flight and were to take the aircraft to London where they would be replaced by another crew. The crew members themselves and their carryon baggage were not subjected to any security checks; however, their checked-in baggage was screened in the same manner as other baggage.<sup>8</sup>

## Montreal

Air India Flight 181 from Toronto arrived at Mirabel International Airport at about 2100 EDT (0100 GMT, 23 June) and parked in supply area number 14 at 2106 EDT (0106 GMT). The 65 passengers destined for Montreal along

---

<sup>8</sup> Bob Rae. (2005). *Lessons to be Learned on Outstanding Questions with Respect to the Bombing of Air India Flight 182*, Ottawa: Air India Review Secretariat.

with three Air India personnel deplaned and were transported by bus to the terminal building. The remaining passengers remained on board as transit passengers and were not permitted to disembark at Montreal. Air Canada baggage handler's off-loaded four containers of cargo, three containers of baggage and a valuables container.

Two diplomatic pouches from the Indian High Commission in Ottawa were delivered to the aircraft by MEGA International Cargo. One pouch weighing one kilogram was hand-delivered to the flight purser for storage in a valuables locker within the cabin and the other pouch was loaded into the valuables container. At about 1730 EDT (2130 GMT), Air Canada, which is Air India's contracted agent, opened its check-in counter to passengers who would be flying on Air India Flight 182. Burns security personnel were also assigned at this time to screen the checked baggage. Passenger tickets were checked, issued a number, and copies of the tickets were removed and retained by Air Canada. Boarding passes were then issued and affixed to the numbered tickets. Also attached to the ticket booklets were numbered tickets which corresponded to each piece of checked baggage. The numbered checked baggage was sent to the baggage area by Air Canada personnel to be security-checked by Burns security personnel. The passengers for AI 182 after checking in were free to enter the departure area. At the entrance to the departure area, Burns security staff used X-ray units and metal detectors to screen passengers and carry-on baggage. At about 2100 EDT (0100 GMT), the passengers proceeded to gate 80 where they gave their boarding passes and numbered tickets to an Air Canada agent. The agent kept the numbered flight tickets and checked the numbers against the passenger list. Also, at gate 80, a secondary security check was done on passengers by a Burns security officer using a metal detector. Hand-carried baggage was subjected to further physical and visual checks. A total of 105 passengers boarded the flight at Mirabel Airport; there were no interline passengers. Between 1900 (2300 GMT) and 1930 EDT (2330 GMT), Burns security personnel identified a suspect suitcase using the X-ray machine. The suitcase was placed on the floor next to the machine. The Burns security supervisor told Air India personnel that a suspect suitcase had been located and was advised within 15 to 20 minutes to wait for the Air India security officer who would be arriving on the flight from Toronto. Subsequently, a second suspect suitcase was identified and a little later a third. The three suitcases were placed next to the X-ray machine. Between 1930 (2330 GMT) and 1945 (2345 GMT), all the Burns security personnel at the X-ray machine were assigned to other duties and the three suspect



suitcases remained in the baggage area without supervision. At about 2140 (0140 GMT), the Air India security officer went to the baggage room and inspected the three suitcases with the X-ray machine and a sniffer that was in the possession of the security officer. The Air India security officer decided to keep the three suitcases and, if further examination proved negative, send them on a later flight.

At approximately 2155 (0155 GMT), the Air Canada Operations Centre supervisor contacted the airport RCMP detachment regarding the suspect suitcases. At about 2205 (0205 GMT), an RCMP member located the suitcases in the baggage room and requested that an Air India representative be sent to the baggage room. About five minutes later, the Air India security officer contacted the baggage room by telephone and advised that he could not come to the room immediately. The Air India security officer arrived in the baggage room at about 2235 (0235 GMT) and, when asked to determine the owners of the suitcases, informed the RCMP member that the flight had already departed [2218 (0218 GMT)]. The three suspect suitcases were later examined with negative results. The remainder of the checked baggage which cleared the security check was identified by a green sticker. The baggage was then forwarded to Air Canada personnel who loaded the baggage in containers to be placed on board the aircraft. A later check with Canada Customs and Air Canada at Mirabel revealed no unclaimed baggage associated with AI 181/182. A similar check at Dorval Airport was conducted with negative results. No record was kept as to the location and number of individual pieces of checked-in luggage. Records were kept as to the location of the containers according to destination, where loaded and the number of pieces of luggage in each container. The Mirabel Detachment of the RCMP provided the following security at the airport on 22 June 1985:

- one member in a police vehicle for airside security;
- one member on patrol in the arrival and departure areas;
- one member on general foot patrol throughout the terminal; and
- one member as a telecommunications operator in the detachment office.

In addition, due to the increased threat to Air India flights, the RCMP provided the following supplementary coverage to Air India Flight 181/182 on 22 June 1985:



- one member in a police vehicle escorted the aircraft to and from the runway and the terminal building and remained with the aircraft while it was stationary;
- one member in a police vehicle remained at the entrance to the ramp;
- two members patrolled the area of the ticket counter and access corridors, and one of these members also served in a liaison capacity with the airline representatives.<sup>9</sup>

### **Pan Am Flight 103**

There was an explosion in the forward cargo compartment which caused an explosive decompression that led to the in flight breakup of Pan Am Flight 103. The combined effect of the direct and indirect explosive forces was to destroy the structural integrity of the forward fuselage. This disaster occurred as a result of a bomb, an improvised explosive device, being placed within a Toshiba radio situated in a brown Samsonite suitcase. The location of the suitcase established that it was an interline bag; namely it had come from another carrier and had been placed on the Pan Am flight at some point in its journey. From its location, it was established it could only have been loaded on the airplane at Frankfurt, Germany. Furthermore, the baggage tags led to a precise paper trail which established that the bag in question was an interline transfer bag from Air Malta Flight 180. The unaccompanied bag was placed on Pan Am 103 A, a feeder flight, and was transferred to Flight 103 at Heathrow Airport, outside London. The bags transferred from Pan Am 103A were taken directly from that aircraft to Pan Am 103, and that they were not counted or weighed. Additionally, they were not reconciled with the passenger manifest, and they were not x-rayed at Heathrow. Thus the bag, which was loaded at Frankfurt, traveled to London and was loaded on Flight 103 without being identified as an unaccompanied bag. Additionally, two Libyans, including the Libyan Arab Airlines station manager at Malta, who had unlimited access to the baggage area for all Air Malta flights were investigated. Libyan Airlines used the same baggage tickets as Air Malta, and on December 21, 1988, the Libyan Airlines flight to Tripoli was processed at the same time and at the same counter as Air Malta Flight 180. Moreover, the security procedures at Malta were symbolic at best.

---

<sup>9</sup> AAIB Aircraft Accident Report No 2/90, Pan Am 103, 22 December 1988, Boeing 747; NAVAVNSAFECEN Investigation 69-67, RA-5C,

## **FAA Security Requirements (overseas) pertinent to Pan Am crash**

Positive passenger baggage reconciliation was long recognized as an important element in the system designed to prevent the carriage of unaccompanied bags. Unaccompanied bags were a well-established method used by terrorists to get bombs on board airline flights. The Federal Aviation Administration (FAA) required a positive match of bags to boarding passengers in airports which were classified as extraordinary security risks airports. Frankfurt and London had been categorized by the FAA as falling into that category. Under FAA rules, once an unaccompanied bag was identified at one of the high risk locations, it could only be carried on board an aircraft if physically searched. Pan Am had abandoned this positive matching process without written approval in February 1987, at Heathrow and in July 1988, at Frankfurt. Without permission from the FAA, Pan Am had substituted what they described as an administrative match and positive passenger control. The new administrative match and positive passenger control system was inadequate because it did not deal with interline bags. Pan Am was aware of their duty to meet the FAA Regulations. The rule was contained in their manuals as required by law. The decision to ignore the rule was taken at the highest corporate level.<sup>10</sup>

### **Warnings/Issue**

In April 1988, the FAA warned all international airlines of intelligence reports of threats by Iran against United States targets. On November 18, 1988, Pan Am was advised by an FAA Security Bulletin that a Middle Eastern terrorist group had been found in Germany with a bomb concealed within a Toshiba radio. The alert called upon Pan Am and other airlines to activate extra vigilance and a rigorous adherence to their regulations for baggage reconciliation. Pan Am and others were warned of the difficulty of relying on x-rays which would not detect such bombs. Despite this explicit warning, Pan Am did not positively match interline bags, even worse, the ALERT security staff in Frankfurt was not made aware of this warning. Not even the personnel using the x-ray equipment were told of this warning. They did not know, and were unaware of what to look for. On December 7, 1988, only two weeks before the Lockerbie disaster, Pan Am was issued a Security Bulletin advising that the United States Embassy in Helsinki, Finland, received a warning that a Pan Am flight from Frankfurt to the United States would be the target of a bomb. The notice became known as the Helsinki

---

<sup>10</sup> AAIB Aircraft Accident Report No 2/90, Pan Am 103, 22 December 1988, Boeing 747; NAVAVNSAFECEN Investigation 69-67, RA-5C,

Warning. It referred to and reiterated the FAAs earlier warning of a Toshiba radio bomb and again emphasized the difficulty of detection by x-ray. Once again the security personnel at Frankfurt, including ALERTs chief of training, were not informed of the bulletin. Pan Am not only failed to increase security staff, they failed to alert the on duty security staff to the warnings. When he eventually received the Helsinki Warning, the manager at Frankfurt attempted to back date it and to suggest that he had disseminated it. He had not.

## **Frankfurt**

Pan Am had their own security and baggage handling staff. There was a computer controlled automated baggage handling system. Each item of baggage was placed in an individually numbered tray as it was taken into the system. The trays were placed on conveyor belts and instructions were fed into the computer to identify the flight to which the baggage was to be sent, the position from which the aircraft was to leave and the time of the flight. The trays were dispatched to a waiting area where they circulated until an instruction was fed in to summon the baggage for a particular flight, whereupon the items would be automatically extracted from the waiting area and sent to the departure point. Local origin baggage was received at check-in desks, and passed into the system. Transit baggage was taken to one of two areas, known as V3 and HM, where it was fed into the system at points known as coding stations. There were seven coding stations in V3. The general practice was that baggage from an incoming flight was brought either to HM or to V3 in wagons or containers and would be directed by an employee called the interline writer to one or more of the coding stations. The proper practice was that each coding station should not deal with baggage from more than one incoming flight at a time. Normally there were two employees at each coding station. One would lift the items of baggage from the wagon or container and place each item in a tray. The other would enter into the computer, in a coded form, the flight number and destination for the outgoing flight, taking the information from the tag attached to the item. Records were kept identifying the staff working at particular stations, the arrival times of aircraft, the arrival times of consignments of baggage at HM or V3, and the station or stations to which the baggage from a particular flight was sent. The computer itself retained a record of the items sent through the system so that it was possible, for a limited period, to identify all the items of baggage sent through the system to a particular flight. The computer controlling the baggage handling system contained its own clock, which had a tendency to diverge from real



time. It was reset at the start of each day, but by 1600 or 1700 hours the discrepancy might be as much as two or three minutes. Times entered in records not generated by the computer were obtained by the staff from the airport clock or from their own watches.

Pan Am had x-ray equipment at Frankfurt, which was used to x-ray interline baggage. The practice of Pan Am at Frankfurt was to carry out reconciliation between local origin passengers and baggage and online passengers and baggage, to ensure that every such passenger who had baggage on the flight was accounted for, but there was no attempt to reconcile interline passengers and their baggage. Flight KM180 reached its parking position at 1248 hours on 21 December 1988. It was unloaded by employees of the airport authority. According to the record, the unloading took place between 1248 and 1300 hours. Andreas Schreiner, who was in charge of monitoring the arrival of baggage at V3 on that day, recorded on the interline writer's sheet that one wagon of interline baggage from flight KM180 arrived at V3 at 1301 hours. A coder, Yasar Koca, was working at station 206 in V3. He completed a worksheet which showed that one wagon of baggage from flight KM180 was coded at station 206 between 1304 hours and a later time which the trial court held to be 1310. No passenger on flight KM180 had an onward booking from Frankfurt to London or the United States. All the passengers on the flight retrieved their checked-in baggage at their destinations. The Malta documentation for flight KM180 did not record that any unaccompanied baggage was carried. There was, however, evidence that there was an item of baggage which was neither accompanied nor otherwise accounted for. A computer printout relating to baggage sent for loading onto flight PA103A bore to record that an item which had been placed in tray number B8849 was coded at station 206 at 1307 hours and was transferred and delivered to the appropriate gate to be loaded on board flight PA103A. There was a plain inference that an unidentified and unaccompanied bag traveled on flight KM180 from Luqa airport to Frankfurt and there was loaded on flight PA103A. Flight PA103A departed for London at 1653 hours. The Air India crash procedures in effect at the time of the incident represent, in conjunction with Lockerbie, failures in the interline security protocols.



## Legal Issues

### International Standards and Recommended Practices

International security standards and recommendations to safeguard international civil aviation against acts of unlawful interference are listed in ICAO Annex 17 to the Convention on International Civil Aviation. Suggested security measures and procedures are amplified in the ICAO Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference.<sup>11</sup> Annex 17 requires contracting States of which Canada is one to “take the necessary measures to prevent weapons or any other dangerous devices, the carriage or bearing of which is not authorized, from being introduced by any means whatsoever, on board an aircraft engaged in the carriage of passengers.” In addition to other recommendations, Annex 17 recommends that contracting States should establish the necessary procedures to prevent the unauthorized introduction of explosives or incendiary devices in baggage, cargo, mail and stores to be carried on board aircraft. These proposals arose from a decision taken by the Council in its 115th Session on 10 July 1985. The Council instructed its Committee on Unlawful Interference, as a matter of urgency, to review the entirety of Annex 17 and to report on those provisions which might be immediately introduced, upgraded to Standards, strengthened or improved. Among the proposed amendments is the following upgrading in the Standards: - Each contracting State ensures the implementation of measures at airports to protect cargo, baggage, mail stores and operator’s supplies being moved within an airport to safeguard such aircraft against an act of unlawful interference.

### Canadian Law

In terms of Canadian statutory requirements, the Civil Aviation Security Measures Regulations and the Foreign Aircraft Security Measures Regulations made pursuant to the Aeronautics Act require specified owners or operators of aircraft registered in Canada or specified owners or operators who land foreign aircraft in Canada to establish, maintain, and carry out security measures at airports consisting of:

---

<sup>11</sup> Convention on International Civil Aviation. Suggested security measures and procedures are amplified in the ICAO Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference, Annex 17.

- systems of surveillance of persons, personal belongings, baggage, goods and cargo by persons or by mechanical or electronic devices;
- systems of searching persons, personal belongings, baggage, goods and cargo by persons or by mechanical or electronic devices;
- a system that provides, at airports where facilities are available, for locked, closed or restricted areas that are inaccessible to any person other than a person who has been searched and the personnel of the owner or operator;
- a system that provides, at airports where facilities are available, for check-points at which persons intending to board the aircraft of an owner or operator can be searched;
- a system that provides, at airports where facilities are available, for locked, closed or restricted areas in which cargo, goods and baggage that have been checked for loading on aircraft are inaccessible to persons other than those persons authorized by the owner or operator to have access to those areas;
- a system of identification that prevents baggage, goods and cargo from being placed on board the aircraft if it is not authorized to be placed on board by the owner or operator; and
- a system of identification of surveillance and search personnel and the personnel of the owner or operator.

Specified carriers including Air Canada, CP Air, and Air India were required to provide a description of their security measures to the Canadian Minister of Transport. An Order-in-Council on 29 September 1960 established that the RCMP was responsible for the direction and administration of police functions at major airports operated by Transport Canada. The duties of the Police and Security Detail at these designated airports include the following:

- carry out policing and security duties to guard against unauthorized entry, sabotage, theft, fire or damage;
- enforce federal legislation;
- respond to violations of the Criminal Code of Canada, Federal, Provincial, and Territorial statutes, and perform a holding action pending arrival of the police department having primary criminal jurisdiction;
- man guard posts; and provide a police response in those areas of airports where pre-board screening takes place. Section 5.1(9) of the Aeronautics Act stated that "The Minister may designate as security officers for the purposes of this section any persons or classes of persons who, in his opinion, are qualified to be so designated." Pursuant to this section Transport Canada has established criteria for persons or classes of persons that are designated as security officers in a Schedule registered on 11 April 1984. The criteria also specify that a security guard company and its employees will meet Transport Canada requirements provided that the company:
  - is under contract with a carrier to conduct passenger screening under the Aeronautics Act and Regulations;
  - is licensed in the province or territory;
  - complies with the security guard criteria as follows in that the guard must:
    - be 18 years or older,
    - be in good general health without physical defects or abnormalities which would interfere with the performance of duties,
    - be licensed as a security guard and in possession of the license while on duty, and

- meet the training standards of Transport Canada consisting of successfully completing the Transport Canada passenger inspection training program, attaining an average mark of 70 per cent, and undergoing refresher training within 12 months from previous training;
- uses a comprehensive training program which has been approved by Transport Canada and is capable of being monitored and evaluated;
- keeps records showing the date each employee received initial training and/or refresher training and the mark attained; and
- provides supervision to ensure that their employees maintain competency and act responsibly in the conduct of searching passengers and carry-on baggage being carried aboard aircraft.<sup>12</sup>

### **Canadian Security Procedures**

In accordance with the Canadian Aeronautics Act and pursuant regulations, air carriers are assigned the responsibility for security. Transport Canada provides the following security services for the air carriers using major Canadian airports, including the international airports in Vancouver, Toronto and Montreal:

- security and policing staff including RCMP airport detachments;
- specific airport security plans and procedures;
- secure facilities (e.g., secure areas, pass identification systems, etc.); and
- security equipment and facilities (e.g., X-ray detection units, walkthrough metal detectors, hand-held metal detectors, explosive detection dogs).

---

<sup>12</sup> *Canadian Air Transport Security Act Statutes of Canada*



- As of 22 June 1985, the following general security measures were in place at Canadian airports:
- metal detection screening of passengers; and
- X-raying of carry-on baggage.

Checked baggage was not normally subject to any security screening. A few air carriers such as Air India had extra security measures in place because of an assessed higher threat level

On 23 June 1985, Transport Canada required additional security measures to be implemented by all Canadian and foreign air carriers for all international flights from Canada except those to the continental United States. These measures required:

- the physical inspection or X-ray inspection of all checked baggage;
- the full screening of all passengers and carry-on baggage; and
- a 24-hour hold on cargo except perishables received from a known shipper unless a physical search or X-ray inspection is completed. Further, on 29 June 1985, Transport Canada directed that all baggage or cargo being interlined within Canada to an Air India flight was to be physically inspected or X-rayed at the point of first departure and that matching of passengers to tickets was to be verified prior to departure.<sup>13</sup>

### **Air India Security Program in Canada**

In accordance with the Foreign Aircraft Security Measures Regulations, Air India had provided the Minister of Transport with a copy of its security program. It included measures to:

- establish sterile areas;
- physically inspect all carry-on baggage by means of hand-held devices or X-ray equipment;

---

<sup>13</sup> Bob Rae. (2005). *Lessons to be Learned on Outstanding Questions with Respect to the Bombing of air India Flight 182*, Ottawa: Air India Review Secretariat.

- control boarding passes;
- maintain aircraft security;
- ensure baggage and cargo security; and
- off-load baggage of passengers who fail to board flights.

Under these procedures established by Air India, passengers, carry-on baggage, and checked baggage destined for AI 181/182 on 22 June 1985 were subjected to extra security checks. A security officer from the Air India New York office arrived in Toronto on 22 June 1985 to oversee the security operation at Toronto and Montreal. On 17 May 1985, the High Commission of India presented a diplomatic note to the Department of External Affairs regarding the threat to Indian diplomatic missions or Air India aircraft by extremist elements. Subsequently, in early June, Air India forwarded a request for "full and strict security coverage and any other appropriate security measures" to Transport Canada offices in Ottawa, Montreal and Toronto, and RCMP offices in Montreal and Toronto.<sup>14</sup>

### **PD-4 Sniffer/Issue**

On 18 January 1985, prior to the inaugural Air India flight out of Toronto on 19 January, a meeting on security for Air India flights (Toronto) was held with representatives from Transport Canada, RCMP and Air India. At this meeting, a PD-4 sniffer belonging to Air India was produced. It was explained that it would be used to screen checked baggage as the X-ray machine had not yet arrived. At that time, an RCMP member tested its effectiveness. The test revealed that it could not detect a small container of gunpowder until the head of the sniffer was moved to less than an inch from the gunpowder. Also, the next day the sniffer was tried on a piece of C4 plastic explosives and it did not function even when it came directly in contact with the explosive substance. It is not known if this was the same sniffer used on 22 June 1985.

### **US Law/FAA Regulations**

Prior to 9/11 air carriers had the responsibility to prevent and deter carriage of weapons and explosives aboard their aircraft by potential hijackers. Where applicable, air carriers issued and carried out written

---

<sup>14</sup> Ibid

security programs, which accomplished 100 percent screening of all passengers and searched all carry-on items.<sup>15</sup> Post 9/11, this basic concept has been expanded to require all baggage be screened by explosive detection equipment before 31 December 2002, not by airlines but by the government. Conversely, airports serving applicable air carriers are responsible for preventing and deterring unauthorized access to the air operations area, and for providing law enforcement support at passenger screening stations. Basically, Federal Aviation Regulation, Parts 107 and 108 required airport operators and airlines to issue a security program incorporating the above procedures. Overall, the FARs set the general guidelines for all security assets and procedures at US airports and for US and foreign airlines servicing US airports.

## Police Support

On 1 April 1981, the FARs were amended as Sec 107.15 to state: Each airport operator shall provide law enforcement officers in the numbers and in a manner adequate to support

1. Its security program; and
2. Each passenger screening system required by Part 108 or Sec 129.25 of this chapter. 49 CFR Chapter XII Part 1544.217, (Nov 2001) requires each airport operator to arrange for law enforcement personnel meeting the qualifications and standards specified in Section 1544.21 and provide its employees current information regarding procedures for obtaining law enforcement assistance at that airport. Basically, it means that law enforcement personnel should be made available within a reasonable period of time.

## Passenger and Baggage Screeners

The sterile concourse establishes an area to which access is controlled by the inspection of persons and property in accordance with an approved security program. Passengers have come to accept them as the normal course of business in an airport. At most airports, security operations are located at a central screening point at the central access point to a concourse, which serves several gates. This negates the need for

---

<sup>15</sup> FAR Part 121.538 and Part 108.7. Note: Current regulations are contained in 49 CFR Chapter XII, Parts 1540 et al.

airport authorities to bear the costs of maintaining security personnel at each gate or to station a law enforcement officer at each gate. This simple change of location from the gate to the choke-point before the concourse entrance eventually made the practicality of x-ray machines to search baggage practical. The cost of an x-ray machine at each gate was a severely costly proposition. X-ray screening only became practical with the improvement of technology and the increase in number of businesses manufacturing them.

Now all sorts of x-ray machines and walk-through or hand held metal detectors have resulted in a tremendous economy of equipment and personnel. Fewer pieces of equipment and, more importantly the need to employ fewer people to operate them, has arguably furnished the greatest savings. Cost related problems have however resurfaced with the high cost of explosion detection systems and the requirement to screen all checked baggage by the end of 2002. It has become clear that airport baggage areas, not the ticket counters, provide a better venue for the location of the newly mandated explosive detection equipment. This will require extensive renovations to some airports. However, placing the explosive detection equipment in the baggage area makes the screening invisible to the passenger and eliminates unnecessary congestion at the check-in and passenger screening points. This sequence becomes part of the normal process of transferring the baggage from the ticket counter to the airplane.

In the past, a vast majority of the people operating baggage and passenger screening systems in airport terminals were contract security guards. The airlines hired airport security firms to conduct essential searches and passengers depended on their expertise to maintain the safety of airports and aircraft around the globe. They were poorly trained and poorly paid, often only receiving minimal training. Their training often consisted of instruction on the operating systems and procedures by someone simply employed longer than the new employee. The instructor or supervisory employee probably did not have very extensive experience, considering most contract firms experienced a 100% turn over rate per year or more. Demographically, they were young, women, retired and/or are representative of a minority segment of the population. Frequently, English or French was their second language. It was ironic that the public relied so heavily on the dedication of these people for their safety and security but failed to reciprocate with appropriate compensation in order to attract more qualified personnel.



In Canada, CATSA immediately began the process of hiring and training personnel to man the security stations at airports. They were faced with the same problems which previously challenged private security firms. In the US, the TSA, is facing those same problems. It now operates most of the US passenger screening process and is tasked with analyzing threats that pertain to the entire transportation infrastructure, aviation related and otherwise. In the US, the GAO had published a report in 2000 clearly portraying the inadequate security previously provided. The report indicated that turn over among personnel was a huge problem. Specifically, the report stated that, "from May 1998 through April 1999, screener turnover averaged 126 percent at 19 of the nation's largest airports."<sup>16</sup>

In another report dated December 2000, The Department of Transportation's Inspector General stated that too many airport employees with unknown or questionable backgrounds are given access to secure areas. "Randomly pulling workers' files at six airports, investigators determined that 16 percent had undergone incomplete background checks and 8 percent had no checks at all."<sup>17</sup> Years previously, there had been some additional alarming studies on the need for improving security at US airports. In 1987, an FAA evaluation at major airports discovered that screeners missed approximately 20% of the potentially dangerous items which passed in front of them. Another study revealed the chilling statistics that screeners in European airports detected twice as many test objects as US screeners. A FAA report concluded that, "people who had longer training, somewhat better pay and benefits, and better on-going testing by screening companies, had much better performance in detecting objects than comparable screeners in the US."<sup>18</sup> In addition, the caretakers of security at airports, unfortunately, were not above being bribed, engaging in criminal activities or just being non-committed to the job. These circumstances often resulted in significant laxness in security. The situation has not really changed all that much in spite of 11 September. Security at London's Heathrow Airport was overhauled in March 2002 after two multi-million dollar heists in a two-month period. The British government announced more stringent background checks on employees, tighter restrictions on access to sensitive areas and now

<sup>16</sup> Sweet, Kathleen. (2003). *Aviation and Airport Security: Threats and Safety Concerns*, Upper Saddle River, NJ: Prentice Hall Publishers, pg 209.

<sup>17</sup> Morris, Jim, "Since Pan Am 103, a Façade of Security", *U.S. News*, 19 February 2001, Internet: <http://www.usnews.com/usnews/issue/010219/safety.htm>, Pg. 1-3.

<sup>18</sup> Rochelle, Carl, "FAA Calls for Security Improvements at US Airports", Internet: [http://www.cnn.ru/2000/travelnews/01/07/bomb\\_and\\_baggage](http://www.cnn.ru/2000/travelnews/01/07/bomb_and_baggage), 7 Jan 2000.

requires security companies to be on an approved list. The job as an airport security guard was not one that children aspired to become while growing up. As mentioned, more often than not, the job paid poorly, provided little chance for advancement or promotion and most likely provided little training for those that were even somewhat dedicated to the job. On top of that, the screeners were frequently subjected to verbal abuse by passengers, airline employees, allegedly by government personnel and by their own co-workers. In fact, a report cited this abuse as the most regularly cited cause of leaving the job, as opposed to low pay and virtually no benefits. It is fair to assume that Canada suffers from these same problems.

Poor operator performance continues to be another principal weakness of passenger screening systems. Airport security screeners, who are preoccupied with inter-personal problems on the job and poorly trained, are still required to identify sometimes faint indications of infrequently appearing target items. Missing such indicators can have catastrophic results if a bomb or other explosive device survives the screening process. This problem will remain and will prove challenging to authorities. The relationship between pay and performance is not necessarily a determinative one. Experts would argue that increased pay is not likely, in and of itself, to solve the problem. The government must place a renewed emphasis on attaining job effectiveness goals. This process will likely involve the application of two types of factors. Those factors will consist of those that attract and keep people on the job (maintenance factors) and those that lead to acceptable or enhanced performance on the job (performance factors).<sup>19</sup>

Another challenge relates to the self-perception of people hired in this field. Higher levels of pay will possibly make up for poor working conditions, but do not enhance the perceived low status of the job. Improved training techniques will greatly improve this aspect. Even the weekly access to "intelligence" briefings on the assessed threat by qualified personnel will improve job satisfaction. People who believe they are actually important and contributing to combating a real threat will often live up to the challenge. Those employees referred to as "rent-a-cops" will not.

---

<sup>19</sup> Guzzo, R.A., 1988, *Productivity in Organizations*, Jassey-Bass: San Francisco, CA.

The use of trace detection technologies and explosive detection systems will also require specialized training. Trace detection equipment requires the use of specific protocols to be effective. Additionally, passenger screening settings may involve person to person contact or direct contact between the equipment and the passenger. Additionally, operators may feel intimidated by passengers. Training regarding the management of anger will also prove quite useful. To facilitate training of screeners, the deployment of a computerized training system called Screener Proficiency Evaluation and Reporting System or SPEARS has proved effective. One unique aspect of the system is a concept known as Threat Image Projection (TIP), which consists of specific software to project fictitious images of bags with threat devices on x-ray screens to keep screeners alert and measure performance in real-time conditions. Governments will likely continue the use of these systems.

It is also important to recognize the distinction between state appointed law enforcement officers and “private” security officers. There are four basic differences. The significant distinctions include financial sourcing, profit orientation, goals toward crime prevention vs. protection of assets and the possession of statutory authority. Private security is employed by profit-oriented businesses. The police are statutorily appointed or sworn-in the service of the public and are paid by governments. Additionally, police officers are often focused on the investigation of crime that has already taken place or is taking place. Private security officers are supposed to focus on crime prevention and the protection of assets belonging to the business. The functions are similar and do overlap but the motivational differences are worthy of note. Furthermore, training for law enforcement in the very complicated airport arena is recommended.

### **Interim Conclusions: Passenger Baggage Reconciliation**

Subsequent to the Air India 182 crash, several recommendations proceeded from the resulting Indian-Canadian reports. One of the most important called for the **complete** reconciliation of all checked baggage to all on-board passengers before flight. This recommendation, however, was never fully implemented for international flights across the industry until the similar loss by explosion of Pan Am Flight 103 over Lockerbie, Scotland, in 1988. Arguably, the issue of cost impinged efforts to correct these problems in 1985. In addition, the reconciliation of passengers to bags for domestic flights was not implemented, in the North American context, until after the events of 9/11. This latter delay was a by-product



of the cost and “operational penalties” associated with the reconciliation of domestic baggage, which is to say that reconciliation takes time <sup>20</sup>

On one end of the spectrum is El Al who, by the time of the Air India 182 incident, had implemented a layered, defence-in-depth security system that put integrated measures in place throughout its operational environment. On the other is the North American civil aviation industry, which, subsequent to the same event, seemed to implement security measures in a reactive, after-the-fact fashion. The reasons for these variations in approach can be related to the balance struck between the perceived need for change and the cost or effort involved in making change happen.

In Canada, the formation of the Canadian Air Transport Security Authority (CATSA) in 2002 became the centerpiece of a reconfigured aviation security system. This development, however, did not seek to address the command-and-control issues that preceded it. The overall system remains fractured. A chief executive officer (CEO) heads the current CATSA system. A Board of Directors oversees the CEO. The board currently comprises 11 individuals, including its chairperson. A dedicated general counsel and three vice-presidents assist the CEO in his responsibilities: there is currently one VP for corporate affairs, one for public affairs, and one for operations. The command-and-control network below this hierarchy is distributed amongst 89 designated Canadian airports. Ten individuals serve as “facilitators” to the nine major or Class 1 aerodromes, while 14 regional managers attend to the remaining Class 2 and 3 facilities (CATSA, 2002). As the Senate Committee for National Security and Defence observed: “A maze-like matrix of departments, agencies and corporations hold responsibilities for security at Canadian airports, and there is a fuzzy Alphonse-and-Gaston relationship between the public and private sector as to who will be responsible if security all goes haywire.” <sup>21</sup> With overlapping and ambiguous responsibilities, the command-and-control arrangements within the Canadian civil aviation security sector need to be revisited.

## Security Requirements

Given the assumed terrorist threat to Canada, Canadian citizens, institutions, and economic capabilities, the existing security systems in

<sup>20</sup> Wallis, Rodney. (2000). *Lockerbie the Story and the Lessons*. Praeger Publishers.

<sup>21</sup> Report of the Standing Senate Committee on National Security and Defence. (January 2003). *The Myth of Security at Canada's Airports*. Second Session Thirty Seventh Parliament.



the Canadian civil aviation industry must present a seamless, coordinated, and effective defence. An effective security organization needs to be able to counter this threat at any point in the operational matrix. This is an onerous task because of the large number of agencies involved and the boundaries that separate them—boundaries that are particularly sensitive to exploitation. An effective security system needs to be able to make plans that address the relevant threats. A relevant threat is one that has both the capabilities and intentions of inflicting damage within the aviation environment; identify the threat before it is able to inflict damage; alert the operational system and organize security forces to react to this threat; direct security forces to engage and defeat the threat; and continuously monitor, test and improve security system capabilities to defeat an adaptable and evolving threat. The making of plans to address the relevant threats presupposes an ability to gather related information and make informed recommendations on how the threats can be defeated.

## Challenges

As stated, the Canadian Air Transport Security Authority (CATSA) administers Canadian civil aviation security responsibilities. A review of the enabling legislation<sup>22</sup> reveals that this agency is having some difficulty in bringing into effect the requirements of a new security system. This legislation indicates that a not-for-profit Crown Corporation is to be primarily concerned with traditional airport security services. These functions revolve around the provision of passenger and baggage screening services with little emphasis on airborne security measures. Indeed, the original CATSA mandate was modified to accommodate the introduction of armed air marshal services as directed by American authorities and as requested by the Air Canada Pilot's Association.<sup>23</sup> The Crown Corporation is remote from publicly-controlled intelligence, enforcement, and regulatory agencies, which will make planning unnecessarily difficult. Likewise, it is not well positioned to identify threats to system security by virtue of its isolation from these same authorities. CATSA authorities are cut off from higher-level public security agencies and are similarly cut off from security providers at the operational level. This is because its enabling legislation authorizes the delegation of responsibility for ground security operations to Local Airport Authorities (LAAs). These agencies, in turn, are permitted to contract services out to private security providers.

<sup>22</sup> Canadian Air Transport Security Act S.C. 2002 c.9.

<sup>23</sup> ACPA, 2001 retrieved at: <http://www.acpa.ca/newsroom>.

Indeed, in the case of airborne security operations no one is in a position to coordinate such activities. This is because the legislation provides no formal channels capable of accommodating such initiatives.

*The facts relating to both crashes provide insight into the threat from passengers checking bags containing explosives and then not boarding the aircraft. Solutions are varied and range in cost from relatively inexpensive to very costly. Hence, policymakers should make decisions on tried and tested risk analysis and risk management approaches.*

## **Risk Analysis Approach**

The classical definition of Risk Analysis is one that describes it as a process to ensure that the security controls for a system are fully commensurate with the risks. The Risk Assessment system should be simple enough to enable its use without necessitating particular security knowledge. This approach enables security to be driven into more areas and to become more evolved. Security should be properly targeted, and directly related to potential impacts, threats, and existing vulnerabilities. Failure to achieve this could result in excessive or unnecessary expenditure. Risk Analysis promotes far better targeting and facilities related decisions.

## **Quantitative Risk Analysis**

This approach employs two fundamental elements: the probability of an event occurring and the likely loss should it occur. Quantitative risk analysis makes use of a single figure produced from these elements. This is called the "Annual Loss Expectancy (AE)" or the "Estimated annual Cost (EAC)". This is calculated for an event by simply multiplying the potential loss by the probability. It is thus theoretically possible to rank events in order of risk (ALE) and to make decisions based upon this. The problems with this type of risk analysis are usually associated with the unreliability and inaccuracy of the data. Probability can rarely be precise and can, in some cases, promote complacency. In addition, controls and countermeasures often tackle a number of potential events and the events themselves are frequently interrelated. Notwithstanding the drawbacks, a number of organizations have successfully adopted quantitative risk analysis.

## **Qualitative Risk Analysis**

This is by far the most widely used approach to risk analysis. Probability data is not required and only estimated potential loss is used. Most

qualitative risk analysis methodologies make use of a number of interrelated elements:

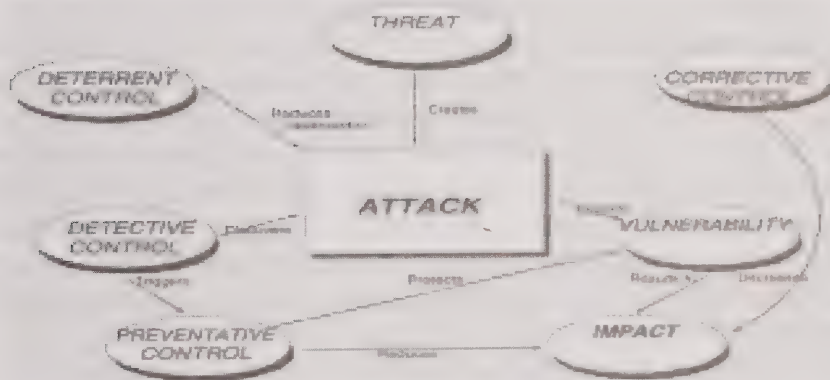
**THREAT:** These are things that can go wrong or that can 'attack' the system. Examples might include fire or fraud. Threats are always present for every system.

**VULNERABILITIES:** These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, for fire vulnerability would be the presence of inflammable materials (e.g. paper).

**CONTROLS:** These are the countermeasures for vulnerabilities. There are four types:

1. Deterrent controls reduce the likelihood of a deliberate attack.
2. Preventive controls protect vulnerabilities and make an attack unsuccessful or reduce its impact.
3. Corrective controls reduce the effect of an attack.
4. Detective controls discover attacks and trigger preventive or corrective controls.

These elements can be illustrated by a simple traditional model:



<sup>24</sup>Sweet 2005

### Tools in the Tool Box

The remainder of this paper will outline a number of countermeasures that can be used to respond to the dangers to aviation security revealed by the Air India and Lockerbie bombings and the methods of risk assessment

<sup>24</sup> Sweet, Kathleen. (2005). Transportation and Cargo Security, Upper Saddle River, NJ: Prentice Hall Publishers.

described above. One theme that will emerge is the appropriate mix of reliance on technology in screening passengers and their baggage in relation to reliance on human judgment and education. The tension between reliance on technology and judgment is underlined by the findings in the Rae report that those who used an explosive sniffer on the Air India baggage were inadequately trained and may not have had the appropriate equipment. A related theme will be the relation between intelligence and interventions aimed at specific passengers and their baggage and interventions aimed at all passengers and their baggage.

A final theme that will emerge is how security improvements in one area such as passenger screening may make other areas such as the planting of weapons on planes by airport staff or placing bombs in baggage more attractive for terrorists and the need for a security system that accommodates for such substitution effects. For example, better screening of passengers and their baggage may also make it more attractive for terrorists to use should fired missiles or use mechanics or other airport staff to sabotage or place weapons on planes.

### **Passenger Profiling**

A profile selectee or random passenger baggage match procedure is an interim solution that could be used until all airlines, to all destinations, could electronically track the passenger lists, boarding passengers and baggage on all flights. Such a system could also be utilized for cruise and rail passengers. The procedure has been the subject of much criticism. If a particular passenger meets the profile, or is selected at random, the passenger's bags receive additional screening both by x-ray and by an explosives detection system when available. This procedure unfortunately does not scan the terrorist who does not meet the profile or is not randomly selected.

A national database on passenger travel habits and history called the Computer Assisted Pre-Screening Passenger System or CAPPS was in use in the US. The original concept proposed a database based solely on travel information; however, it could later be cross referenced with FBI, CIA or criminal records, even though the FAA denies that this was being done. This system establishes some basis for risk assessment and does indeed cut down the risk. At the same time, however, it also assumes that terrorist groups are not very bright and cannot escape the profile that attracts increased attention. Even though profiles are not published,



parameters can be easily guessed. As stated, CAPPs II was highly criticized but should have been recognized, if properly controlled, as a valid tool in the security toolbox.

### **Passenger Protect Program/No Fly list**

The proliferation of government watch lists are a troubling development in the “war on terrorism.” The challenges of such lists include differences of opinion on who’s actually a security threat, consolidating information across agencies by making the computer systems communicate the with one another. Canada’s Auditor General Sheila Fraser found in 2004 that watch-lists used to screen visa applicants, refugee claimants and travelers seeking to enter Canada were in disarray because of inaccuracies and shoddy updating.<sup>25</sup> The challenge is complicated by the vast and growing databases of electronically stored personal information that draw on different agencies’ records, which must be continually updated to be accurate. Agencies and airlines are using computer-driven algorithms to compare travelers’ names against watch lists.

### **Use of Technology- X-Ray-Based Detection Systems Standard X-Ray Scanners**

Standard x-ray scanners have been extensively commercially developed and are available from a number of manufacturers. Units vary in cost, but quality devices range from \$20,000 to \$40,000 per unit. The standard airport hand-baggage scanner has a fan-shaped or scanning x-ray beam that is transmitted through the object to be viewed. The absorption of x-rays is usually measured by a line of detectors, and a high resolution image, derived from the degree of absorption of the beam, is produced. The image depends primarily on the density of objects located in the bag/cargo along the beam of the x-ray. These devices cannot distinguish between a thin sheet of a strong absorber, such as a metal and a thick slab of weak absorber. Simple x-ray systems rely on humans to serve as pattern recognition devices; in the absence of advanced computer pattern recognition techniques, they are very dependent on human factors. *This boils down to the proper training and competency of the screener.*

X-ray scanners are available in single and double monitor versions, with the two views being orthogonal. X-ray scanners can present images

---

<sup>25</sup> Auditor General’s Report March 2004

in up to 80 shades of gray depending on the amount of absorption. Sometimes, the images are presented in a quasi-color where colors are used to produce an artificially enhanced visual presentation. Standard features now include image enhancement, automatic threat alert, full contrast and aspect stretch, high/low density penetration, sensor-free scrolling and automatic edge enhancement plus dual energy features with organic and inorganic stripping displayed on two monitors.

### **Dual- or Multi-energy Scanners**

These devices have also become commercially well developed by several vendors. They are available at approximately \$100,000 per unit. These dual energy systems are actually comprised of two separate x-ray systems whose beams are generated by sources that peak at different energies, producing two independent images. This higher energy view requires less absorption. While areas of heavy elements are dark in both views, areas of light elements are darker in the lower energy projection. By comparing the two images, light elements such as carbon, nitrogen and oxygen may be highlighted. In this way, it is possible to determine whether a given object is made of a light or heavy element. Multi-energy systems are essentially the same except that they have a single x-ray tube that transmits a broad spectrum of energies. Detectors are used to select specific energy regions. These systems then combine to produce effectively the equivalent result.

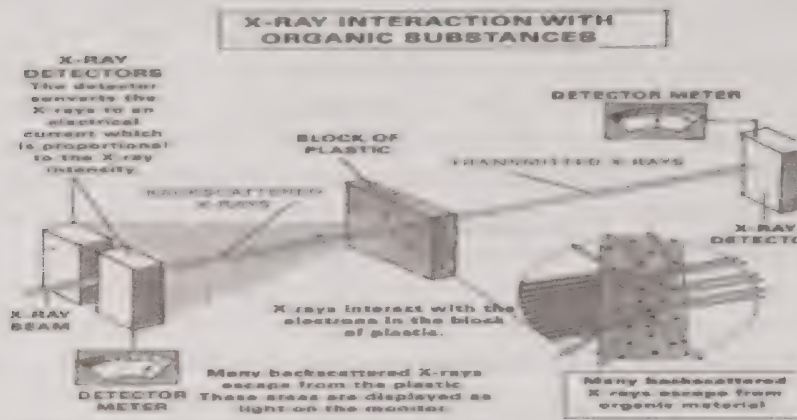
This technique cannot distinguish among the light elements. However, it can overcome the countermeasure of hiding explosives behind an object made of a heavy element, unless enough material is present to absorb the entire beam, which would require an 8-10 mm piece of steel. (I.e. can you hide explosives behind a heavy object with a regular x ray machine discussed above)? These devices are technically identical to a simple x-ray scanner, except for the dual energy and image feature. The systems use color to separate the image into organic, inorganic and opaque materials. The organic consist primarily of light elements, the inorganic of heavy elements and the opaque materials, which would contain a lot of heavy element matter. Explosive materials are made of organic matter and some scanners assign the color orange to organic materials in order to make them more clearly visible.

## Backscatter X-Rays

Backscatter X-rays are also commercially available and use computer algorithms to function in order to automatically detect explosives. Systems are available from between \$60,000 to \$100,000 per unit either as a single or dual viewing system. Most systems scan a pencil beam of x-ray across the object and create two images: the normal transmission image, created by a single detector on the opposite side and a backscatter image, created by a large area detector on the side of the entering beam. A single energy beam is utilized. A two-sided version of this system with two identical x-ray beam systems makes backscatter measurements from opposite sides of the object to enhance the backscatter penetration of the system. The transmitted beam provides a typical x-ray image showing primarily the absorption by heavy elements. Backscatter signal intensity depends on how much of the transmitted beam has been absorbed, how much is backscattered and how many of the backscattered x-rays reach the backscatter detectors. The backscatter signal depends on the competition between photoelectric absorption and Compton scattering. The photoelectric cross section increases with the atomic number of the object, while the Compton cross section is relatively independent of atomic numbers. The resulting backscatter signal favors the low elements with particular emphasis on low elements of high density, including plastic explosives. Backscatter imaging provides a direct measure of the density of elements with low atomic number.

Most manufacturers produce two independent x-ray images: an x-ray transmission image emphasizing the high elements and an x-ray backscatter image emphasizing the low elements. Systems are unique and utilize proprietary techniques.

Companies continue to research a computer algorithm for automatic detection of explosives with the aim of achieving a high probability of detection and a low false alarm rate for explosives. The automatic detection scheme is based on an algorithm that compares properties of bag images against acceptable thresholds. The system builds a database of acceptable histograms by observing and "learning" the characteristics of a large variety of luggage. An algorithm sorts and combines data for online comparison with acceptable values.



Another device produces a virtually “naked” image of passengers by bouncing x-rays off their skin. The device however does enable staff to instantly detect any hidden weapons or explosives. A test program started in (2004) is still underway at London’s Heathrow Airport, Terminal 4. As discovered previously during a test at Orlando Airport in Florida in 2002, the graphic nature of the black and white images has raised some concern about the privacy of passengers. In the US, the deployment of such equipment has been delayed until the developer can refine a method to mask the passenger’s modesty. At Terminal 4 in London, the trial is being conducted jointly by British Airports Authority and the Department of Transportation.

If the body scanner is able to cope with large volumes of travelers, improves detection and receives public acceptance, it will likely be deployed throughout Britain. Passengers are currently selected to go through the body scanner on a random and voluntary basis. Those who decline are subjected to hand search. The scanner resembles a large filing cabinet and is operated in a curtained area. Once screened, the images are automatically deleted. Security officials are pleased with its effectiveness because it detects the outline of any solid object, which conventional metal detectors might be likely to miss. Managers are citing the positive aspects of the ability to avoid intrusive hand searches. Regardless of its effectiveness, passengers are still a bit startled by the clarity of the image. This technology as application for passengers and bags.

26 Electronic Privacy Information Center, Transportation Agency’s Plan to X-ray Traveler’s Should be stripped of Funding. (June 2005) Retrieved from: <http://www.epic.org/privacy/surveillance/spotlight/0605/>



## **Computerized Tomography (CT) (Baggage only)**

This system represents an adaptation of a compact, fast and mobile medical CT scanner. The main difference between the two types of use (security at airports and medical diagnosis) is that the machines used in transportation facilities have more shielding to stop the scattered radiation where, in medicine, the patient is not shielded. The concept utilizes a conventional x-ray scan projection to locate areas with sufficient density to represent a possible threat. In addition, multiple detectors placed on a rotating circumferential element around the object, measure the transmitted signal from a fan beam that traverses it. The density at each location along the path of the beam can be determined, with the rotating action giving the information to provide a complete two-dimensional slice. The inspected object is moved through the detector beam by means of a conveyer belt, providing the third dimension i.e. multiple slices then creates a computer projection with good spatial resolution.

The system operates and looks like a medical scanner or medical CAT computerized axial tomography scanner. The explosive detection device was adapted based on the same principles. The system first produces an x-ray scan similar to the conventional x-ray scanner. An automated inspection algorithm determines the locations within the baggage where the absorption indicates a suspicious area; cross-section CT slices then need to be made to determine the density, texture, mass and shape of the object. Dual-energy CT, a theoretically possible, although not yet implemented option, would also provide information on the nature of the explosive. If no high-density areas are detected, a single slice through the bag is made to look for any sheet explosives that may not have been seen in the projection scan. Since the CT scan produces true cross sectional slices, it is able to identify objects that are surrounded by other materials or hidden by innocuous objects. When alarms are encountered, the CT Scan operator can make further slices to reveal size, shape, mass and make-up of the suspect object. Three dimensional rendering may also be applied.

## **Trace Detection**

Trace detection may be best known for its explosives detection capabilities. Trace detection refers to a group of products that can analyze a swipe or air sample, detecting and identifying minute traces of substances. Some

equipment can access the human convection plume, a natural airflow phenomenon radiating from the human body, to collect any threatening particles. The plume moves upward and predetermined flow rates help the hood capture optimal information. If someone has explosives strapped to their bodies or has even handled explosives, those trace particles will contaminate clothing and register. The machine uses the plume as the vehicle to capture the sample and send it to the detector hood.

The process takes four seconds to collect the trace particles and another 8 seconds to analyze it. A proximity sensor activates both visual and audio prompts for the passenger to enter. As the person stands in the center of the archway, gradually stronger puffs of air come from four surrounding columns positioned to direct them from the lower to the upper body parts of the body, accelerating the plume at a faster rate than it would naturally rise. The plume is collected in the overhead detector and collected particles are vaporized. The molecules are either positively or negatively charged to become ions, which are pulsed down a drift tube. The equipment measures in milliseconds how fast the ions travel from point to point. This acts as the thumb print of the substance, since each specific type of ion has its own particular travel time. This enables the machine to identify a broad range of organic matter, including explosives. The systems also perform high speed baggage inspection to accurately measure mass, density, atomic number and other physical characteristics of objects, providing three independent x-ray images of each bag. Using algorithms software, the MVT can pinpoint the direct location of suspect items to decrease the time length of the search. The MTV's belt speed of 100 feet per second scans 1800 bags per hour, as opposed to airport screeners that process bags at a rate of 400-500 per hour. The MTV is approximately three times cheaper than current scanners, costing about \$500,000 per unit. As regards the Ion Track Itemiser, it uses ion trap mobility spectrometry (ITMS®) technology. It is extremely simple to use. The surfaces of a vehicle or luggage that are suspected of being tainted with contraband are wiped down with a paper disk known as a sample trap. The trap is then inserted into the desktop analyzer. Once analyzed, the contraband substance is identified, along with its relative alarm strength. Visual and audible indications are provided, and the analysis can be stored and printed for later use as court-accepted evidence.

In late October 2004, the TSA deployed an explosive detection trace portal from Smiths Detection of Pine Brook, N.J. at JFK International Airport in Terminal One. It was to remain deployed for at least 90 days during

the pilot program. Rear Admiral David M. Stone, Assistant Secretary of Homeland Security for TSA used the deployment as means to reiterate that the TSA is committed to using cutting edge technology. The passenger walks through portals similar to metal detectors. Puffs of air are blown at passengers and samples are then collected and analyzed for explosives. If the portal's alarm sounds, the passenger and or property are screened more intensely. This type of machine had already been deployed at T.F. Green State Airport, Providence, R.I., Greater Rochester International Airport, San Diego International Airport, Tampa Florida International Airport and Gulfport Biloxi International Airport.

On 22 September 2004, the TSA also announced the deployment of some related technology. They deployed a new Explosives Trace Detection Document Scanner that can "sniff" passenger documents such as boarding passes and drivers' licenses for traces of explosives at several major airports. The airports are Los Angeles International (LAX), New York's John F. Kennedy (JFK) and Chicago's O'Hare International (ORD). "TSA is committed to deploying new explosives detection technologies to passenger security checkpoints to safeguard the traveling public," said Rear Admiral David M. Stone, USN (Ret.), Assistant Secretary of Homeland Security for TSA. "TSA continues to lead the way in utilizing the latest emerging technologies with various pilots to screen both passengers and air cargo for explosives."<sup>27</sup> The pilot program was first unveiled, a few weeks prior, at Ronald Reagan Washington National Airport. Tests were conducted for a minimum of 30 days at each airport. The Document Scanner analyzes samples collected by swiping the surface of a document over a collection disc and alerts the screener if explosives residue is detected. During the pilot, passengers selected for secondary screening at particular checkpoints had their boarding passes scanned. If the Document Scanner alarms, additional screening procedures are implemented. This pilot is one in a series of next-generation tools being tested by TSA including explosives trace detection portals, which are being tested in four airports with nearly a dozen more to come online in the near future.

## Quadruple Resonance

Quadruple resonance uses carefully tuned pulses of low intensity radio waves that probe the molecular structure of targeted items, such as

---

<sup>27</sup> TSA News Release, <http://www.tsa.gov/public/display?theme=44&content=09000519300cf9c8>



explosives or narcotics. The waves momentarily disrupt the alignment of targeted nuclei, which produces a characteristic signal picked up by a receiver and sent to a computer for rapid analysis. "The signal emitted by the explosive or drug is unique," says Lowell J. Burnett, president and CEO of Quantum Magnetics Inc., a subsidiary of InVision. "Specialized radio frequency pulse sequences have been developed for the optimal detection of such explosives as Semtex, C-4, Detasheet, TNT, tetryl, ANFO, and black powder, and such narcotics as cocaine or heroin."

## Metal Detectors

Previously, passengers were required to pass through simple metal detectors before boarding a vessel or aircraft or entering a facility or sterile concourse. However, such efforts have been repeatedly found to be less than 100% effective. There are still easily recognizable deficiencies in many current metal detectors. They simply do not trap all forms of dangerous weapons. More often, their greatest weakness is often cited as the inability to detect metals incapable of being magnetized. Since a significant number of US manufactured guns are made of nonferrous metals, the shortfall is quite evident. They also can not detect the organic materials contained in explosives. Regardless, metal detectors remain one of the most important sources of security for transportation facilities. Additionally, there have been significant advances in equipment which include software programs that can suppress ferrous detection while boosting non-ferrous metals. Others suppress non-ferrous materials while magnifying the detection response of ferrous objects.

The scientific principle upon which metal detectors work is quite simple. Passive systems detect metal by changes in the earth's magnetic field. Active detectors operate by creating an electro magnetic field and alarming when the field is disturbed by metal objects passing through it. Metal detectors contain one or more inductor coils that are used to interact with metallic elements on the ground. A pulsating current is applied to an internal coil, which then induces a magnetic field. When the magnetic field of the coil moves across metal, the field induces electric currents called eddy currents. The eddy currents induce a magnetic field which generates an opposite reaction in the coil, which induces a signal indicating the presence of metal.<sup>28</sup> Standard features now include improved target discrimination, increased throughput traffic

---

<sup>28</sup> "How a Metal Detector Works", <http://micro.magnet.fsu.edu/electromag/java/detector> pg 1. 24 July 01.



flow, advanced signal processing, lower false alarm rates and higher threat object detection rates. Regardless, problems have continued even in the use of these relatively simple machines. For example, in 2002, for the second time in a three year period, a metal detector was accidentally unplugged at Logan International Airport, triggering a security breach that prompted the evacuation of 750 passengers and delayed 11 flights.

## **Selecting a Metal Detector**

The selection of an appropriate metal detector is an important decision to be made by transportation facility and mode of transportation officials. Each facility has its own unique characteristics and priorities. Unfortunately, one of the primary limitations is usually cost and metal detectors can be expensive assets that need maintained and routinely upgraded.

Additionally, the accuracy and utility in the passenger environment of each detector is a weighty aspect. The growing demand for security at access points has moved technology toward walk-through and hand-held metal detectors. The rapid flow of passengers is of major concern to airlines seeking to keep their balance sheets on the positive side of the ledger. In order to keep on making money, the various components must keep the passenger relatively agreeable to the delays caused by screening 100% of the terminal or station traffic. Equipment causing too many false alarms, breaking down on a repeated basis or otherwise causing delays is not marketable in these venues.

In order to satisfy market demand, many companies have been through innumerable successive generations of equipment. Those improvements have featured increased levels of security performance in metal detection capability, discrimination of personal metal objects, and immunity to outside interference. Safety precautions regarding the passenger with a life support device have also been tested and re-tested to protect the operator and manufacturer from civil liability.

Of course, the bottom line for each metal detector is whether or not it actually accurately detects guns and dangerous weapons. The actual detection rates are for security reasons not published. Suffice it to say they must possess a high detection rate. Today's hardware and software programs improve interference rejection, discrimination, sensitivity, detection, uniformity, vibration tolerance and orientation response. All of these factors contribute to the bottom line that increased discrimination

significantly reduces unwarranted alarms. Many metal detector manufacturers now also sell enhancement programs that help correct detection non-uniformity caused by vertically positioned external metal. Other programs allow the user to create customized security programs. Additionally, the proficiency of the operator is also a critical factor.

The manager circumnavigating the hundreds of pages of marketing materials on metal detectors still has to consider some basic concepts in determining the most appropriate system for their particular use. Overall, managers need to contemplate such issues as external factors or sensitivity to environmental factors (i.e. environmental magnetic noise); Physical construction or size; Ease of Operation, (i.e. ease of calibration, self calibration, and required frequency of calibration) and last but not least cost and appearance.

Additionally, development has produced machines, which now have a multi-zone advantage. In addition to indicating the location of targeted objects, multi-zone systems have a multitude of advantages. They improve discrimination between weapons and harmless objects, reduce unwanted alarms and permit higher traffic flow rates. In high volume airports this translates into lower operating and capital costs. For example, pin-point multi-zone detection is a concept formerly pioneered by Ranger. The manufacturer uses a "block of real estate" example to explain the dynamics of the system. They explain that in "most detectors the blocks of real estate, called zones, are stacked upon each other and extend the full width of the archway. When an object passes through a zone, it is detected by the zone and an alarm display shows its location. In this case, the alarm display depicts the height of the object above ground. The display can take the form of lights on the front edge of a side panel or a mimic display that represents the archway in graphic form."<sup>29</sup>Manufacturers do place different interpretations on the meaning of multi-zone detection. Appropriately, when a device claims to have 6 horizontal zones, it should mean that there are twelve detection channels with two sensors per zone. Each zone should be independently adjustable.

False alarms are attributable to external electrical and electro-magnetic interference and poor tolerance vibration. Good quality interference

---

<sup>29</sup> Defining Multi Zone Detection: Check Apple for Apples", <http://www.omni-security.com/wthru2/wtindex.html>, pg. 2, 3 May 2001

rejection and mechanical design will lower false alarms. Multi-zone detectors reduce unwanted alarms caused by people literally wearing metal; jewelry, coins, keys etc. Two conditions contribute to elevated undesired alarm rates. They include the cumulative signal effect and non-uniform detection. Cumulative signal effect lowers a detector's ability to separate weapons from harmless personal effects. It occurs when signals generated by metal are processed as a single composite signal. Theoretically, in single zone machines, the signals from someone's watch, their keys and some metal in their shoe will be combined. If the cumulative signal is large enough, the machine will alarm causing delay and frustration for passenger and screener alike.

Correspondingly in multi-zone detectors, if the device has 18 zone detectors, six horizontal zones would be divided into three blocks. The machine would then display the object's height above the ground, and also show if the object was to the right or left or in the center of the zone. Complicated mapping algorithms process the data and can very accurately tell the scanner where the object is. Because each zone has an adjustable control, the sensitivity can be focused and a particular object for a better analysis thereby making a threat assessment easier and reducing unwarranted alarms.

Another feature to consider before purchasing a specific piece of equipment is the information the screener receives from the alarm panel during an alarm. The alarm panel should show the height at which the detected object is carried. For example, more advertised zones are not necessarily better unless the numbers of horizontal sensitivity controls are present to adjust those zones. This is arguably more important than the actual number of zones. This significantly cuts down on the time needed to actually locate a weapon if there is one. Furthermore, the equipment should be continuously active, have self-testing diagnostics and a fast automatic reset. Electrical and electro-magnetic interference rejection can be achieved through multiple frequency selection, electronic filtering and sophisticated software algorithms.

### **Hand Held Body Scanners**

The best hand held detectors are light weight in construction, have a comfortable grip and a large scanning surface. The detector should have a tight detection pattern, fast detection circuitry and be ergonomically designed. These attributes contribute to higher efficiency and reduced



operator fatigue. Another really useful feature is a switch which can transform the detector from a general use mode to a super high sensitivity unit capable of detecting very small masses of metal.

They should generally have been able to detect a Medium pistol at 12 "(300mm); a Small pistol at 9" (230); and a Razor Blade at 3" (25m) and should scan about 3" to 24" per second. They also need to be adjustable. For example, the controls should enable to the scanner to lower the sensitivity to avoid unwanted alarms for small harmless objects like key chains. Sensitivity adjustments are usually made through a screwdriver access hole in the handle. Most quality devices encase the circuitry in a rugged high impact case which should detect both ferrous and non ferrous metals and alloys. It should be capable of not alarming when the scanner is used to screen at ankle height and in the vicinity of re bars in the floor.

Alarms are both visual and audio. They should remain activated while the search coil is over a metal object. The duration of the alarm is usually indicative of the size of the object. Most use alkaline batteries in a power source which should last at least 80 hours. Low voltage conditions, like cell phones, should advise the user that the power is low. The average weight is a pound or less. Visual only alarm indications are advisable if a weapon is detected. The screener can simply ask the individual to step to the side for the moment, giving security personnel time to respond accordingly. An audio alarm also alerts the perpetrator that they are "trapped" and they may respond accordingly. Generally, as stated no more than 15% of the people who alarm the detector should be false alarms. In other words, no more than 15 unarmed passengers out of 100 should alarm the detector.

### **Interim Conclusion: Equipment**

Screening of passengers and their baggage on all sorts of modes of transportation, in conjunction hopefully with future cargo screening, will continue way into the 21<sup>st</sup> Century. How intrusive the measures can become before the public rejects the level of intrusion will be dependent upon the threat as it is perceived by the traveling public and not necessarily the government. Technological advances continue to be made and improvements in technology will equate to improvements in security. The better the equipment the more reliable the results, as long as the supervisors of screeners train them appropriately.



It is an international offense to “knowingly and willfully” enter an aircraft or airport area in violation of security requirements and yet millions of people try it. So called security experts even boast what they carry on in a concealed manner; trying to make the whole process into a joke. Such conduct, misconduct if you will, exhibits unprofessional conduct and does not further the safety and security of the traveling public. The penalty for having weapons in a secure area is stiff and include up to 10 years in prison, with or without a separate fine especially if the prosecution can prove you intended to commit a felony, like hijacking. It is possible to receive a sentence of a year imprisonment simply for breaching security. If an individual is apprehended actually carrying a weapon onto a vessel, similar to the British journalist who smuggled a meat cleaver and a dagger onboard a flight out of London’s Heathrow Airport, it is possible under UK and US law to be imprisoned for 10 years to life.

The CATSA/TSA systems have been plagued with the same problems as the former private security companies that manned the machines. They were supposed to put safety first. That is, they were not supposed to put passenger convenience and flight schedules ahead of security. Such was the primary reason why legislators had “federalized” the airport-screening workforce and created the new agencies in the weeks after the September 11 attacks. No longer would airport security be left to minimum-wage workers, employed by and answerable to the airlines.

But after five years and billions of dollars, former and current screeners from numerous airports around North America continue to report that procedures are routinely violated to accommodate the airports’ and airlines’ business needs. According to the screeners, luggage is often loaded onto planes without being screened for explosives, and passenger checkpoints are regularly understaffed, increasing the risk of guns and knives being smuggled aboard. The bottom line, they say, is that screeners, under pressure from the airlines, has loosened its security practices to eliminate hassles for passengers and, in doing so, has seriously compromised safety. If this is true, all the technological improvements in the world will not improve security at transportation facilities.

The transition process for security operations since September 11, 2001 has not been smooth, but much progress has been made. However, transportation security is still a “work in process.” New technologies being developed will significantly affect many of the operations in place today. Depending on the changing nature of system threats and the tolerance of the public to intrusion levels, transportation security equipment will

continue to evolve. Cargo screening in particular will be improved. In fact, it must be or a similar catastrophic event might occur similar to the Air India or Lockerbie tragedy or worse.

### **Bomb Sniffing Dogs**

Dogs have a great sense of smell. Their noses are about 100,000 to a million times more sensitive than a human's nose and a well-trained dog can detect up to 20 different kinds of explosives. Furthermore, the legality of their use is well established and do not seem to be significantly limited by civil liberty type legislation. Dogs disclose only the presence or absence of illicit substances and nothing more. They are less intrusive than a typical search and the limited disclosure exposed the property owner to a minimum amount of inconvenience.

Canines are also less expensive than other means of explosive detection. Dogs costs about \$6000 to train and a piece of equipment can cost more than a million dollars. Currently, dogs are generally only used at airports if the threat of a bomb is eminent. Bomb sniffing dogs are not without their problems, which include short attention spans, false alarms, sickness, and distraction of female dogs in heat. To pass the normal certification test, the dogs must receive a score of 100% accuracy. They must convince the handlers that they can successfully detect at least 20 known explosive compounds, which enables them to identify over 19,000 varied explosive combinations. Their training system is based on a food reward program. The method rewards the dog for detecting a compound. To re-enforce the conditioning, they are never fed without some exposure to an explosives' odor. This keeps the dogs highly motivated to sniff out the explosive, because food is always available if they do. The ATF and the US Department of State have provided dogs and training to numerous airport authorities around the world. The program was successfully used by the Australians before the 2000 Olympic Games and has been in operation at high threat airports for a number of years. Dogs are compact, mobile and capable of working in a variety of environments including confined spaces. More importantly in the airport environment they can reduce the manpower needed to screen huge quantities of cargo.

### **Hiring and Good Management**

Hiring, normally within the purview of a department of human resources, is actually the most critical element in establishing a good security program.

All references should be checked and all educational qualifications should be confirmed. Candidates should also sign a document swearing to the fact that they have never been convicted of a felony. As confirmation of the truth of that statement, criminal background and history checks should be conducted through local, state, federal and international authorities where suitable. It is also recommended that psychological examinations be utilized. Additionally, it is very important that human resources administer tests certifying each candidate possesses adequate communication skills to include the basic ability to communicate verbally and in writing in an appropriate language prior to hiring. Previous employment history should be verified as well as actual contact made with all listed references. Lastly, pre employment and regular drug screening procedures need to be a mainstay of the program. These basic hiring criteria are even more critical if the security officers are to be armed during the course of employment. All initial hires should be advised of a discretionary probationary period during which they can be dismissed for any reason.

## **Indoctrination**

Exposure to the CATSA philosophy and mission is important but even more so is a security awareness attitude that is instilled into the new employee from the very first day of employment. Standards of minimum acceptable conduct must be supplied to the employee and they should sign a document indicating they understand those standards. The employees should also be made aware of the uniqueness of working within the transportation system milieu and the potential consequences of a lapse in security. Other standard orientation subjects should include thorough instruction in procedures and policies, emergency response techniques, report writing, legal authority and familiarity with equipment usage.

As mentioned, the employee should be briefed on the utilization of a random drug screening program and that they are subject to testing on a constant basis. They should be made aware of the fact that failure of such a test will result in loss of employment. A drug rehabilitation program is not an appropriate alternative to employees within a security function. Another disqualifier is for new employees to fail the training provided during orientation. Unsuitable candidates can usually be easily identified and replaced before being placed in the work setting. Officers should be able to review the facilities overall master security plan. Additionally, a



security manual with a set of operational instructions (IO) should exist and be reviewed. Compliance with the IO's should result in adequate security for the facility with specific responsibilities clearly detailed.

## **Training**

Employee training should always contain immediate advisement of the objectives of the training. Employees should know what body of knowledge they are expected to retain upon completion of the training. Training which does not conclude with a test often leads to a lax attitude toward the training. The ultimate goal of training is higher job performance on the job. Non retention of the material nullifies the period of instruction and is a waste of employee paid time. Furthermore, a trained officer is much less likely to make errors which could result in a loss.

The question of whether to train staff in situ or send them to an off site training course is always a determination of cost, availability and quality. Off site courses may or may not coincide with facilities schedules and or budget. If on-site training is chosen, the instructors should be certified and competent.

## **Access Control**

Access control restricts the ability of unauthorized individuals from gaining access to a specific area. Access control systems assure the proper identification of personnel across multiple facilities and locations on a selective basis, to secure areas. In 1000 BC the Chinese required servants at the Imperial Palace to wear rings engraved with unique intricate designs identifying palace areas they were permitted to enter. Historians credit this method by the Chinese as the first comprehensive access control system.<sup>30</sup> Advancement in science and technology has improved on the Chinese system. Some systems can also be programmed to lock and unlock access points at specific times and on specific days.

The best equipment should also maintain detailed records of movement through secured areas. The coded information can record time of access, zone accessed and duration of access. There are two basic types of access control devices- the card reader and the code transmitter. These devices read magnetically coded information on a card or a small transmitter emitting a continuous signal which is worn by the user. The information

---

<sup>30</sup> John Naudts, "Access Control; It's in the Cards", Security Management, 1987, pg 169



is transferred to a computer that compares the received information with a database. If the information does not match, the system can be programmed to alarm. Computers have brought much more sophisticated approaches to access control systems.

To keep official documents, uniforms and vehicles out of the hands of terrorists, most security experts suggest the following protective measures:

Keep comprehensive records of all official identification cards, badges, decals, uniforms and license plates distributed, documenting any anomalies and canceling access for items that are lost or stolen.

Practice accountability of all vehicles to include tracking vehicles that are in service, in repair status, or sent to salvage.

Safeguard uniforms, patches, badges, ID cards, and other forms of official identification to protect against unauthorized access to facilities, to include stripping all decommissioned vehicles slated for resale and/or salvage of all agency identifying markings and emergency warning devices.

Check multiple forms of valid identification for each facility visitor.

Verify the legitimate business needs of all approaching vehicles and personnel.

Improve identification card technology to eliminate reuse or unauthorized duplication.

Alert uniform store vendors of the need to establish and verify the identities of individuals seeking to purchase uniform articles.

Ensure all personnel are provided a security briefing regarding present and emerging threats.

Encourage personnel to be alert and to immediately report any situation that appears to constitute a threat or suspicious activity.

Arrange for law enforcement vehicles to be parked near entrances and exits.

Limit the number of access points and strictly enforce access control procedures.

Institute a robust vehicle identification program, including but not limited to checking under the undercarriage of vehicles, under the hood, and in the trunk.

Provide vehicle inspection training to security personnel.<sup>31</sup>

Computers have revolutionized access control systems. The use of voice recognition systems, signature recognition, retina recognition, hand geometry and fingerprint recognition has all expended biometric technology to be a cost effective and highly accurate alternative to cards.

All aviation related systems should require that access control systems must:

1. Enable only those persons authorized to have access to secured areas to obtain that access.
2. Immediately deny access at the access point to individual's whose access authority has changed.
3. Have the capability of zone coding, so that it can admit or deny access by area.
4. Have the capability of time-coding, being able to admit or deny access by time and date.

## Barriers

The primary function of a barrier is to delay the intruder as much as possible and to force him to use methods of attack that are more conspicuous and noisy. As the value of the target increases, however, the strength of the barrier must increase proportionately. The trade-off between delay time and detection time is perhaps the single most important consideration in designing a barrier. Some facilities are protected by a natural barrier, such as the water surrounding Alcatraz. Usually, however, a barrier must be constructed as a physical and psychological deterrent to intruders. Fences, define the site perimeter, briefly delay an intruder, channel employees and visitors to authorized gates, keep honest people out and serve as a sensor platform. Barriers such as a chain link fence have the

---

<sup>31</sup> Retrieved from : <http://www.identicard.com>.

added advantage of being able to see through it, where solid walls block security's view and the intruders view.

Perimeter barriers, according to the NCPI are, "any obstacle which defines the physical limits of a controlled area and impedes or restricts entry into the area. It is the first line of defense against intrusion... At a minimum a good perimeter barrier should discourage an impulsive attacker."<sup>32</sup>

## Smart Cards

Today, Optical Memory Cards and smart card technology is the way of the future. They possess one or more integrated circuit chips capable of storing a great deal of information and interpreting it. Each card must authenticate identity and contain a photograph and microchip when the holder logs onto a computer or enters a facility. However, smart cards are very complicated entities. It is just this complexity which might doom them in the market place. They require sophisticated microprocessors and exhaustive authorization procedures. An even newer technology might replace them.

None of these cards provide effective security in the wrong hands. The card does not know who is holding it and the machine reading the signal or data does not know either. An access card can simply not identify a specific individual using the card. It is only wishful thinking to assume that every time a card is used that the person using it is actually the person authorized to use it. As mentioned previously, piggy backing is also a problem. One person opens the door or access point and several people follow them through. Another issue arises when terminated employees fail to turn in their security badges, but some companies are attempting to rectify this problem with cards that expire.

## Biometrics

Employees should all need to enroll their fingerprints or some other unique physical trait into a database. Biometrics have progressed a long way since the first models appeared on the commercial market. The information stored in biometric system databases are usually the name, ID pass number and the fingerprint or other trait of the employee into a template. The process of enrollment takes about 5 minutes. The employee

---

<sup>32</sup> National Crime Prevention Institute, *Understanding Crime Prevention*. Stoneham, MA., Butterworth Publishers, 1986)

can access restricted zones by presenting their ID cards to a proximity reader which acknowledges the employees ID number. They then place their finger, hand, retina or face onto or near the biometric scanner. A signal is sent from the scanner to the biometric database, requesting that it reconcile the badge number with the imprint. In the matter of two seconds the equipment recognizes the employee and displays green or rejects the possible intruder. International biometric standards are currently being developed.

Access to the database must be restricted to designated personnel and must be inaccessible outside the facilities network. Biometric information must be encrypted. Systems will not only improve the level of access control but will also reduce the risk of identity fraud while increasing confidence in security. Generally, biometric systems are designed to recognize biological features of individuals in order to facilitate identity verification. There only drawback is that in today's modern medical world, physical characteristics can be changed. Currently, the following types are available commercially.

- a. Fingerprint- optical scanning of a finger which is matched to a database.
- b. Signature recognition- relies on the fact that individuals write with distinct motion and pressure. Forgers can duplicate the appearance but not the style.
- c. Hand geometry- utilizes the physical attributes of the hand such as the length of fingers.
- d. Speaker verification- utilizes the uniqueness of voice patterns.
- e. Eye retina- analyzes the blood vessel pattern of the retina.

### **Closed Circuit Television CCTV**

Closed circuit television has become the most common security device in many applications, not just along a perimeter. Their sophistication may range from simple fixed black and white monitoring cameras to infrared capability. They can be used in corridors, entrances and secured areas to name just a few. Cameras can instantly monitor activity near a fence and record the intruder if needed. Some are even equipped with motion



detectors to alert a guard that a camera has detected an individual near the fence. They have become indispensable in today's security world and come in all shapes, sizes and budget requirements. A significant enhancement to CCTV came with digitization. For example, now a QUAD can compress images from four cameras into a single frame of VCR tape or DVD, allowing the operator to view all four cameras on a four way split screen. Video multipliers also allow the system high speed, full frame recording from multiple sources. Infrared cameras now also can be used for night surveillance. Newer systems provide sharp images of distant subjects at high frame rates with remarkably reliable recording apparatus. The number of cameras one officer can control is theoretically unlimited but in reality, the more cameras the less time spent on each view. The International Professional Security Association Security Instruction and Guidance Manual recommend the following:

**Sequential switching-** fixed cameras are sequentially switched to a single monitor and the operator has a view of each location in turn.

**Motion switching** – a fixed camera that covers a static scene can be made to switch to the monitor if any movement is detected by the lens.

**Combination-** the sequential switching is interrupted if a camera detects some motion within the field of view and the image is presented on the screen.

**Manual control-** the operator is able to switch each camera into the monitor screen as required.

**Multi-screen-** several small screens simultaneously display the images from the various cameras: used where the cameras are rotated, tilted, zoomed, etc. by the operator. Often a picture of interest can be switched to a larger screen for detailed examination. The quality of recorded images must be very high so that people, objects and vehicles can be identified. Highest quality is required especially when the subject occupies only a small fraction of the camera field of view because the image must be enlarged to see the subject. Images require not only high numbers of pixels, i.e. the full native resolution of high quality, CCTV cameras, but also have high sharpness and few compression artifacts. For this, high data rates are needed unless the frame rate is extremely low, but a low frame rate reduces the chance the subject is video photographed facing the camera and that no objects block the view.

Improved capture of the images of moving objects is needed since transportation platforms or passengers are often moving. Video cameras should have progressive scan, rather than the common interlaced scan of broadcast TV. The problem is that cameras with interlaced scan require two interdigitated snapshots for each full-frame image, one for the even scan lines and one for the odd scan lines. Subjects often move during the time that elapses from the first half of snapshot to the next, blurring the combined image. The use of progressive scan rather than interlaced scan often gives the increased sharpness equivalent to an exposure period that is reduced by ten-fold for a subject that occupies a fraction of the height of the image.

The video security system for transportation systems should be able to do a first level of screening of the video captured in real time to reduce the amount of manpower required to identify potential threats. The motion detection algorithms used in stationary systems, where the camera is affixed to the wall of the building are not adequate because the only motion is motion of potential subjects, not motion of the platform, i.e. motion of a train or ship, and thus movement of the camera. It must be possible to communicate live images in real time from both mobile and fixed platforms to security personnel who are stationed on them. Requiring the use of only powerful desktop and notebook computers with a high-speed local area network is too restrictive a requirement for viewing live and recorded images from multiple cameras simultaneously.

Finally, since video, access control, biometric and other sensor systems must be integrated together to form a total security solution, the video security system should be designed so that it can easily be integrated into other systems.

## **Alarms**

Should the fence, barrier or wall be circumvented, alarm systems are the next line of defense. Alarms can be silent, audible or visual. Visual alarms are specifically designed to catch someone's attention to a potential problem. A blinking red light is the classic example, either on a control panel console or at the site of the alarm involved. Audible alarms are intended not only to alert security but also to scare the intruder. Silent devices are designed to alert security as well as law enforcement if desired.

## Lighting

Adequate lighting on the perimeter is also a mandatory security function. The spread of the light should be directed outward from the fence line. This will illuminate the approach of an intruder and also obstruct the intruder's view. If closed circuit television is part of the perimeter protection scheme, the placement of the cameras and lights must be coordinated. Careful attention should be paid to not creating areas of shadow and glare; preventing an unobstructed view.

## An Integrated System of Access Control

The number of gates providing access should be limited to the number of essentially required entry points. Gates either need to be guarded by security officer or constantly viewed by some sort of electronic equipment, either CCTV or by use of a card actuation system to gain access. Earlier methods involved simply padlocking the gate and providing keys to only those truly needing them. Advances in technology enable security now to utilize electronically generated controls, key card access, keypad access and others depending on the budget of the operation. Dogs are also a viable option.

A fence provides minimal protection. Lighting adds to the protection level. However, the combination of a fence, proper lighting, and at least two sensors greatly increases the probability that an intruder will be detected. Sensors can be expensive, and the actual threat must be weighed against the cost. Sensors in alarm systems range from simple magnetic switches to sophisticated Doppler radar. Alarm systems vary but all have three basic common elements.

- A. an alarm sensor
- B. a circuit or sending device
- C. an enunciator or sounding device

In choosing a system, the object, space or perimeter to be protected is the very first consideration after which an analysis of the intensity and frequency of outside noise, movement or potential interference must be factored into a final decision.

## Summary

Most countries have taken a “legal” or “criminal” approach to prosecuting terrorists. They assess the results of an attack and pursue a public legal remedy based on the specific misconduct already deemed criminal in a standard penal code context. Murder, kidnapping and assault by terrorists are treated exactly the same as murder, kidnapping and assault by any other type of criminal. Other sovereign nations have chosen to create the offense of terrorism. They have legislated laws, which apply directly to the anti-terrorism effort. Some have been in place for quite a long time as in Northern Ireland and the Middle East. Others like those enacted in Canada to combat the FLQ have been short-lived. Like in all other criminal cases, the legislation is subject to review by the judiciary and is bound by the fundamental civil rights dictated. Other countries are not held by those same constraints.

Many nations have tried many remedies to control terrorist activity. New technologies become available with increasing speed to assist authorities in providing security at airports and onboard aircraft. However, all of these available technologies used by security personnel or anti-hijacking/rescue squads must be viewed in perspective and in the proper focus. Technology is not the bottom line. The human effort behind the security demands scrutiny as well. The current political sentiment has justified massive budget expenditures to militaries, police forces and other agencies. Such actions also have challenged constitutional personal rights to travel, to privacy and equal protection under the laws. It is clearly within every nation’s best interests to harness the concern for airline safety. The key is to do so within acceptable democratic norms.

Each airline determines what procedures are appropriate for its own operation. In the recent past, however, the airlines have all come to realize that the threat is very real. Additionally, that very real threat has made it clear that security is cheap in comparison to the costs of a major security breach. The airlines have been forced to think the unthinkable. Namely that the cockpit is not secure, the terminal is not secure and the aircraft is not secure unless proper procedures and equipment are used to make them secure.

In accordance with the concept of awareness of the threat, the airlines need to take one step further and recognize that quick stopgap measures will prove to be insufficient. Furthermore, more of the unthinkable



thoughts need to be addressed. Those unthinkable thoughts; including the threat of nuclear, biological or chemical attack will continue to plague the airlines and airports. New procedures and policies must be developed to meet these threats. The ebola virus released in one aircraft and transported thousands of miles across an ocean can potentially kill millions of people.

### **Reference Materials:**

AAIB Aircraft Accident Report No 2/90, Pan Am 103, 22 December 1988, Boeing 747

ACPA, 2001. Retrieved from: <http://www.acpa.ca/newsroom>.

Addis, Karen K., "Profiling for Terrorists," *Security Management*, Vol. 36, No. 5, May 1992.

AirDisaster.com, (nd). Special Report: Air India Flight 182; <http://www.airdisaster.com/special/special-ai182.shtml>.

"Advanced Solutions for Weapon Screening and Asset Protection," Ranger Security Detectors, El Paso, Texas, 2001.

Born, M. and Wolf, E., 1964, *Principles of Optics*, New York.

European Community Radiological and Nuclear Medicine Installations Regulation 1998- Regulation 8

Electronic Privacy Information Center, Transportation Agency's Plan to X-Ray Traveler's Should be Stripped of Funding. (June 2005). Retrieved from: <http://www.epic.org/privacy/surveillance/spotlight/0606/>.

Canadian Aviation Bureau Aviation Occurrence, Air India Boeing, 747-237B VT-EFO Report

Congressional Research Service "The Library of Congress"

Convention on International Civil Aviation, Annex 17.

Defining Multi-Zone Detection: Check Apple for Apples. (3 May 2001). Retrieved from: <http://www.omnisecurity.com/wthru2/wtindex.html>. pg 2,3.

Federal aviation Regulations Part 121Guzzo.R.A. (1988). Productivity in

Organizations, San Francisco, CA: Jassey-Bass.

Hardage, M.L., Marbach, J. R., Winsor, D.W., "The Pacemaker Patient and Diagnostic Device Environment", Modern Cardiac Pacing, Futura Publishing Company, Mount Kisco, NY, pg. 857-873, 1985.

How a Metal Detector Works. (24 July 2001) Retrieved from: <http://micro.magnet.fsu.edu/electromag/java/dectector/>. Pg 1.

Indian Kirpal Report, Report Of The Court Investigating Accident To Air India Boeing 747

Aircraft VT-ETO, "Kanishka" On 23rd June 1985

Ionizing Radiation Regulations 1999, UK, (Statutory Instrument No. 3232)....., "A Performance Evaluation of Biometric Identification Devices", Sandia Corporation, UC-906, June 1991

National Research Council, "Airline Passenger Security Screening, New Technologies and Implementation Issues", Publication NMAB-482-1, National Academy Press, Washington, D.C. 1996.

National Crime Prevention Institute. (1986). Understanding Crime Prevention, Stoneham, MA: Butterworth Publishers.

NAVAVNSAFECEN Investigation 69-67, RA-5C, 14 June, 1967

Naudts. John, (1987). Access Control: It's in the Cards. Security Management, ASIS, pg. 169.

Morris, Jim. (19 Feb 2001). Since Pan Am 103, a Façade of Security. US. News, Retrieved from: <http://www.usnews.com/usnews/issue/010219/safety.htm>. pg 1-3.

Report of the Standing Committee on National Security and Defence. (January 2003). The Myth of security at Canad'as Airports. Second Session Thirty Seventh Parliament . Retrieved from: <http://www.parl.gc.ca/37/2/parlbus/commbus/senate/com-e/defe-e/rep-e/rep05jan03-e.pdf>.

Radiological Protection Act of 1991 Irish Legislation- Section 2  
United Nations Scientific Committee on Effects of Atomic Radiation,

UNSCEAR, "Sources and Effects of Ionizing Radiation, United Nations, NY, 1994.

Bob Rae. (2005). Lessons to be Learned on Outstanding Questions with Respect to the Bombing of air India Flight 182, Ottawa: Air India Review Secretariat. Retrieved from: <http://www.cbc.ca/news/background/airindia/pdf/rae-report.pdf>

Rochelle, Carl.(2000). FAA Calls for Security Improvements at US Airports. Retrieved from: <http://www.cnn.ru/2000/travelnews/01/07/bombandbaggage>.

*STUDIES IN DEFENCE AND FOREIGN POLICY, NUMBER 2* The Fraser Institute  
10 Canadian Civil Aviation Security

Sweet, Kathleen M., *Terrorism and Airport Security*, Edwin Mellen Press, Lewiston, NY, 2002.

Sweet, Kathleen M., *Aviation and Airport Security*, Prentice Hall Publishers, Upper Saddle River, NJ.

TSA News Release. Retrieved from: <http://www.tsa.gov/publuc/display?theme=44&content=09000519800cf9c8>.

Wallis, Rodney. (2000). Lockerbie the Story and the Lessons. Praeger Publishers.

### **Additional Resources**

The recent review by an Independent Advisory Panel of the *Canadian Air Transport Security Authority (CATSA) Act* and the corresponding body it established to implement and manage screening functions at Canada's airports.[http://www.tc.gc.ca/tcss/CATSA/FinalReport-Rapport\\_final/final\\_report\\_e.pdf](http://www.tc.gc.ca/tcss/CATSA/FinalReport-Rapport_final/final_report_e.pdf)

The recent *Special Examination Report* of CATSA by the Auditor General of Canada: [http://www.catsaacsta.gc.ca/english/about\\_propos/rep\\_rap/oag\\_bvg/CATSA%20Spec\\_Exam\\_E.pdf](http://www.catsaacsta.gc.ca/english/about_propos/rep_rap/oag_bvg/CATSA%20Spec_Exam_E.pdf)

A link to the Fifth Estate's investigative documentary, "Fasten Your Seatbelts", on aviation security in Canada: <http://www.cbc.ca/fifth/fastenseatbelts/>

## Biography

I am currently an Associate Professor at the Virginia Commonwealth University and an Adjunct Professor at Embry Riddle aeronautical University and Goodwin College. I formerly taught courses in Aviation Security, Terrorism and Strategic Intelligence in the Department of Aviation Technology at Purdue University. I am CEO and President of Risk Management Security Group and am certified by the UK and Irish Department of Transport to teach air cargo security. I received my undergraduate degree from Franklin and Marshall College in Lancaster, Pennsylvania, in Russian Area Studies and a Master's Degree in history from Temple University. I have been admitted to the bar in Pennsylvania and Texas after graduating from Beasley School of Law in Philadelphia, PA. I am a graduate of many Air Force and civilian training programs.

After graduating from law school, I joined Wyeth International Pharmaceuticals as a legal specialist focused on licensing agreements between Wyeth and international agencies. I later joined the US Air Force and initially was a member of the Judge Advocate General's Department. I frequently served as Director of Military Justice at the base and Numbered Air Force level. After fifteen years as a JAG, and generally engaged in prosecuting cases on behalf of the military, I transferred to the 353rd Special Operations Wing as a military political affairs officer. I was later an intelligence officer assigned to HQ AMC as an executive officer and briefer. In 1995, I became an Assistant Air Attaché to the Russian Federation. As an attaché, I was engaged in liaison work not only with the Russian Air Force but also the Federal Security Bureau, at which time I became interested in counter terrorism efforts.

My final assignment was as an instructor at the Air War College where I taught in the International Security Studies division. I later became an Associate Professor at St. Cloud State University in the Department of Criminal Justice and an Associate Professor at Embry Riddle Aeronautical University; teaching security and intelligence related courses. I am the author of four books, *Terrorism and Airport Security*, (Edwin Mellen Preses, March 2002); *Aviation and Airport Security: Terrorism and Safety* (Prentice Hall Publishers, Nov 2003) and *The Transportation Security Directory* (Grey House Publishing, Jan 2005.) My fourth book, *Transportation and Cargo Security: Threats and Solutions* was published in late 2005.



My company, Risk Management Security Group, doing business in Ireland as RMSG Ireland Ltd., engages in all aspects of consulting in transportation-related security: including the preparation of threat and vulnerability assessments and security awareness training.











Commission of Inquiry  
into the Investigation  
of the Bombing of  
Air India Flight 182

